

УДК 621.39

Б. О. ПАЛКОВСКИЙ (ЭС-31)

Научные руководители: старшие преподаватели *С. В. КИСЕЛЁВА*,
В. Е. МИНИН

АНАЛИЗ УЯЗВИМОСТЕЙ СЕТЕВЫХ ПРОТОКОЛОВ

Проведен анализ сетевых протоколов моделирование в Cisco Packet Tracer и Scapy. Рассмотрены понятия: сеть, сетевой протокол, сетевые модели OSI и TCP/IP(DOD). Также рассмотрены переполнение CAM-таблицы, DHCP-SNOOPING и моделирование DDoS-атаки в Scapy.

Введем основные понятия сети и сетевого протокола:

1 Сеть – это два или более компьютера, соединенных между собой для обмена информацией.

2 Сетевые протоколы – это международные стандарты или конвенции, которые определяют некоторые правила эффективной коммуникации между компьютерами в сети.

Основными сетевыми моделями являются OSI и TCP/IP(DOD) (рисунок 1). В современных сетях используется TCP/IP(DOD) [2].

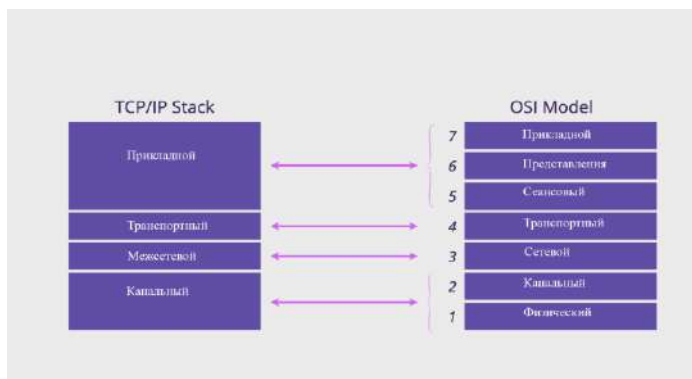


Рисунок 1 – Сетевые модели

Сеть (рисунок 2) представляет собой коммутатор, на который в дальнейшем будем проводить атаку, 3 персональных компьютера (пользователи) и стороннее устройство злоумышленника (также может является пользователем), по схеме видно, что устройство физически соединено в сеть.

Рассмотрим несколько примеров сетевых атак.

Переполнение SAM-таблицы

Коммутатор имеет SAM-таблицу, где содержится привязка MAC-адресов к портам коммутатора (рисунок 3).

С помощью специальных программ можно изменять MAC-адрес, при этом коммутатор воспринимает его как новое устройство и добавляет в таблицу. Далее при переполнении этой таблицы (рисунок 4) коммутатор начинает работать как концентратор и весь трафик будет переходить на остальные устройства, в том числе злоумышленника, и он сможет перехватить конфиденциальную информацию.

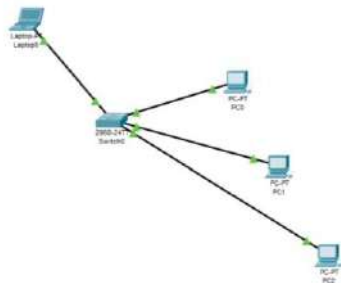


Рисунок 2 – Схема сети

```
Switch#show mac-address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0007.ec4d.8175	DYNAMIC	Fa0/3
1	00d0.d3dd.0dbc	DYNAMIC	Fa0/4

```
Switch#show mac-address-table
Mac Address Table
```

Рисунок 3 – SAM-таблица (до атаки)

Vlan	Mac Address	Type	Ports
1	0007.ec4d.8175	DYNAMIC	Fa0/3
1	000c.cfb8.c2ca	DYNAMIC	Fa0/1
1	0060.7088.6996	DYNAMIC	Fa0/2
1	00d0.d3dd.0009	DYNAMIC	Fa0/4
1	00d0.d3dd.000b	DYNAMIC	Fa0/4
1	00d0.d3dd.000d	DYNAMIC	Fa0/4
1	00d0.d3dd.000f	DYNAMIC	Fa0/4
1	00d0.d3dd.0011	DYNAMIC	Fa0/4
1	00d0.d3dd.0090	DYNAMIC	Fa0/4
1	00d0.d3dd.0110	DYNAMIC	Fa0/4
1	00d0.d3dd.0111	DYNAMIC	Fa0/4
1	00d0.d3dd.0112	DYNAMIC	Fa0/4
1	00d0.d3dd.0113	DYNAMIC	Fa0/4
1	00d0.d3dd.0119	DYNAMIC	Fa0/4
1	00d0.d3dd.011b	DYNAMIC	Fa0/4
1	00d0.d3dd.0186	DYNAMIC	Fa0/4
1	00d0.d3dd.0187	DYNAMIC	Fa0/4
1	00d0.d3dd.0188	DYNAMIC	Fa0/4
1	00d0.d3dd.0189	DYNAMIC	Fa0/4
1	00d0.d3dd.0191	DYNAMIC	Fa0/4
1	00d0.d3dd.0192	DYNAMIC	Fa0/4
1	00d0.d3dd.0193	DYNAMIC	Fa0/4
1	00d0.d3dd.0194	DYNAMIC	Fa0/4
1	00d0.d3dd.0195	DYNAMIC	Fa0/4
1	00d0.d3dd.0196	DYNAMIC	Fa0/4
1	00d0.d3dd.0197	DYNAMIC	Fa0/4
1	00d0.d3dd.0198	DYNAMIC	Fa0/4
1	00d0.d3dd.0199	DYNAMIC	Fa0/4

Рисунок 4 – Переполненная SAM-таблица

Рассмотрим способы защиты от этой атаки. Для начала на рабочие устройства следует установить ограниченный доступ, для того чтобы невозможно было использовать пассивный перехват, например, скачать Wireshark или похожие приложения и тем самым предотвратить возможность просмотра трафика. Еще один способ связан с настройкой самого коммутатора (рисунок 5).

В начале мы переходим в режим конфигурации, затем в конфигурацию портов и указываем, что они будут работать в режиме доступа. Затем мы включаем защиту «port-security». Далее прописываем, что, если к нам подключаться более 3 устройств, сначала порт будет отключен и пошлет соответствующее сообщение.

ние по SNMP и syslog. И таким образом при попытке подключения более 3 устройств, наш коммутатор будет их откидывать. И в конечном итоге первые 3 MAC-адреса, которые будут получены через этот порт, и будут автоматически сохранены в running-config [2].

```
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security vi
Switch(config-if-range)#switchport port-security violation s
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#switchport port-security max
Switch(config-if-range)#switchport port-security maximum 3
Switch(config-if-range)#switchport port-security mac
Switch(config-if-range)#switchport port-security mac-address s
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#exit
Switch(config)#exit
Switch(config)#exit
Switch#
%SYS-S-CONFIG_I: Configured from console by console
show mac address-table
-----
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----
1       0007.ec4d.8175   STATIC    Fa0/3
1       00d0.d3dd.0186   STATIC    Fa0/4
Switch#
%LINK-S-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
Switch#show mac address-table
-----
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----
1       0007.ec4d.8175   STATIC    Fa0/3
```

Рисунок 5 – Настройка коммутатора

В итоге этого хватает для защиты от переполнения CAM-таблицы.

Рассмотрим протокол, защиту и атаку DHCP-SNOOPING.

DHCP – протокол прикладного уровня модели TCP/IP, служит для назначения IP-адреса клиенту. Это следует из его названия – Dynamic Host Configuration Protocol. IP-адрес можно назначить вручную, но если наша сеть довольно большая, тем сложнее это делать и возрастает риск ошибки при настройке. Поэтому для автоматического назначения IP-адресов был создан протокол DHCP [2].

DHCP-SNOOPING. Злоумышленник может сформировать и послать DHCP-серверу огромное количество DHCP-запросов с разными MAC-адресами (рисунок 6). Сервер будет выделять IP-адреса, и в конечном итоге весь DHCP-пул закончится, после этого сервер не сможет обслуживать новые устройства. По сути, это DoS-атака, так как нарушается работа сети. Метод борьбы с подобными атаками называется DHCP Spoofing. Когда коммутатор получает пакет, то он сравнивает MAC-адрес, указанный в DHCP-запросе, с MAC-адресом, который был прописан. Если адреса совпадают, то коммутатор отправляет пакет дальше, если не совпадают, то пакет откидывается.

Злоумышленник может также развернуть свой DHCP-сервер и выдавать свои настройки пользователям сети.



Рисунок 6 – Схема с DHCP-сервером

Для того чтобы на DHCP-запросы отвечал именно сервер злоумышленника, ему необходимо предварительно вывести из строя легальный DHCP-сервер. Практические действия для реализации данной атаки аналогичны представленным в разделе, посвященном переполнению САМ-таблицы (см. рисунок 4). При смене MAC-адреса и перезапуске сетевого интерфейса производится запрос к DHCP-серверу для получения нового IP-адреса.

В DHCP Spoofing существуют доверительные (trusted) и не доверительные (untrusted) порты, первые могут получить DHCP ответ, вторые, соответственно, нет.

Однако к настройке (рисунок 7) ограничений нужно относиться с осторожностью, так как в случае превышения заданного значения запросы будут отклонены. В начале рабочего дня, когда множество пользователей одновременно включает свои компьютеры и получает IP-адреса по DHCP, это ограничение может привести к задержкам и проблемам при входе в сеть.

```
Switch>
Switch>en
Switch>enable
Switch>cin
Switch>con
Switch>conf
Switch>configure terminal
Enter configuration commands, one per line. End with
Switch(config)#ip d
Switch(config)#ip dh
Switch(config)#ip dhcp sn
Switch(config)#ip dhcp snooping
Switch(config)#inte
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 0/1
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#ip dh
Switch(config-if)#ip dhcp sno
Switch(config-if)#ip dhcp snooping t
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)# ip dh
Switch(config-if)# ip dhcp sn
Switch(config-if)# ip dhcp snooping lim
Switch(config-if)# ip dhcp snooping limit 10
^
% Invalid input detected at '^' marker.

Switch(config-if)# ip dhcp snooping limit rate 10
```

Рисунок 7 – Защита от DHCP Spoofing

Перейдем к инструменту Scapy. Scapy (рисунок 8) представляет собой инструмент, написанный на языке Python для работы с сетевыми пакетами [3].

Проведем с помощью Scapy условную DDoS-атаку на систему, работающую на Windows Server 2003, которые до сих активно используются. В этой DDoS-атаке (рисунок 9) происходит отправка большого числа пакетов на адрес получателя (dst=192.168.1.123). В конечном итоге машина, на которую произошла атака, не обязательно зависнет, но замедление работы обязательно случится. Для веб-сервера такая атака может оказаться критичной.



Рисунок 8 – Меню Scapy

Таким образом для современных сетей необходимы постоянный мониторинг, активная защита и настройка оборудования. В этом помогают встроенные механизмы защиты, например, такие как Port Security, DHCP Snooping и т. д.

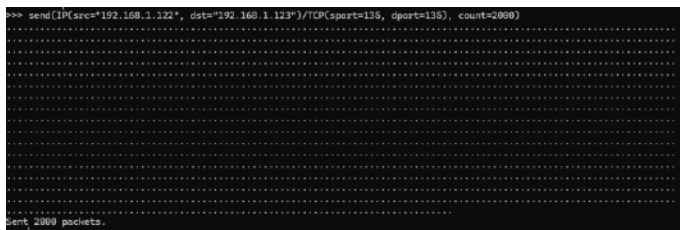


Рисунок 9 – Модуляция атаки

Также необходимы постоянные обновления и установка более нового и стабильного ПО, которое поддерживается, ОС Windows Server 2003 хоть и работает до сих пор, и выполняет свою функцию, но имеет большие проблемы с безопасностью и злоумышленнику не составит большого труда использовать уязвимости. Вместе с этим можно использовать различные инструменты (в данной статье это – Scapy), которые могут наглядно показывать процесс атаки.

СПИСОК ЛИТЕРАТУРЫ

- 1 Мощь Scapy // ХАБР. – URL: <https://habr.com/ru/articles/249563/> (дата обращения: 12.05.2026).
- 2 **Бирюков, А. А.** Информационная безопасность: защита и нападение / А. А. Бирюков. – 2-е изд., перераб. и доп. – М. : ДМК Пресс, 2017. – 434 с.
- 3 **Форшоу, Дж.** Атака сетей на уровне протоколов : руководство хакера по перехвату и анализу сетевого трафика и эксплуатации уязвимостей / Джеймс Форшоу ; пер. с англ. Д. А. Беликова. – М. : ДМК Пресс, 2021. – 340 с.

Получено 17.06.2026