# **Задание 1**

Вы подняли на своём домашнем компьютере с IP-адресом 192.168.0.2 web-сервер.

* Получится ли у пользователей интернета открыть этот сайт?
* Нужно ли будет вам для этого что-то сделать дополнительно?
* Существует ли такой набор настроек провайдера, который не позволит подключение?

Поразмышляйте над примером.

*Приведите ответ в свободной форме.*

# **Решение 1**

Сеть 192.168.0.0/24 диапазон адресов IPv4, принадлежащий к частным сетям, значит это локальная сеть, и сервер с адресом 192.168.0.2 не будет доступен из сети интернет.

Для того, чтобы сделать доступным его для пользователей интернет, необходимо иметь внешний IPv4 адрес, например, на точке доступа или роутере, подключенном к интернет. Потребуется организовать трансляцию Destination NAT и открыть порт на устройстве (прописать port forwarding), которому необходимо назначить “белый” внешний адрес, принадлежащий сети интернет (купить услугу у провайдера). Например, условно, пробросить порт 8080 на внешнем адресе 5.4.3.2 на порт 80 на адресе 192.168.0.2 в локальной сети. Пример команды для iptables:

iptables -t nat -A PREROUTING -p tcp --dport 8080 -i eth0 -j DNAT --to-destination 192.168.0.2:80

Дополнительно необходимо позаботиться о том, чтобы порт на внешнем IPv4 адресе роутера был открыт на межсетевом экране провайдера.

# **Задание 2**

* Узел src инициировал соединение с узлом dst.
* На маршрутизаторе узла src была создана трансляция:

| **src local IP:port** | **src global IP:port** | **dst IP** | **protocol** |
| --- | --- | --- | --- |
| 10.0.0.2:1111 | 93.15.10.2:2222 | 1.1.1.1:80 | tcp |

Применив знания по установке TCP сессий, ответьте на вопросы:

* Сможет ли злоумышленник доставить пакет до 10.0.0.2, отправив пакет на адрес/порт 93.15.10.2:2222 с адреса 74.5.12.4?
* А если злоумышленник подменит source IP-адрес и сгенерирует пакет с source IP:port - 1.1.1.1:80

*Приведите ответ в свободной форме.*

# **Решение 2**

В случае, если настроена трансляция в соответствии с таблицей, обмен пакетами с хоста 10.0.0.2 осуществляется только с IP 1.1.1.1, т.е. пакет с 74.5.12.4 будет отброшен.

Если будет осуществлена подмена, возможна доставка пакета, однако, поскольку TCP протокол использует сессии, злоумышленнику нужно будет перехватывать трафик и подделывать заголовки TCP.

# **Задание 3**

* Узел src инициировал соединение с узлом dst.
* На маршрутизаторе узла src была создана трансляция:

| src local IP:port | src global IP:port | dst IP | protocol |
| --- | --- | --- | --- |
| 10.0.0.2:1111 | 93.15.10.2:2222 | 8.8.8.8:53 | udp |

Применив знания по работе UDP, ответьте на вопросы:

* Сможет ли злоумышленник доставить пакет до 10.0.0.2, отправив пакет на адрес/порт 93.15.10.2:2222 с адреса 74.5.12.4?
* А если злоумышленник подменит source IP-адрес и сгенерирует пакет с source IP:port - 8.8.8.8:53

*Приведите ответ в свободной форме.*

# **Решение 3**

В случае, если настроена трансляция в соответствии с таблицей, обмен пакетами с хоста 10.0.0.2 осуществляется только с IP 8.8.8.8, т.е. пакет с 74.5.12.4 будет отброшен.

Если будет осуществлена подмена, возможна доставка пакета, UDP не использует сессию, и все будет зависеть от конкретной реализации NAT и настроек firewall на пути прохождения пакетов.

# **Задание 4**

Найдите самую часто встречающуюся проблему при работе клиентов за NAT с протоколом FTP, связанную с особенностью работы FTP (на лекции по портам эта особенность упоминалась).

1. В чём выражается проблема?
2. Почему она возникает?
3. Что можно сделать, чтобы избежать этой проблемы?

*Приведите ответ в свободной форме.*

# **Решение 4**

1. Проблема выражается в периодическом разрыве соединения с FTP сервером при работе в активном режиме, если клиент за NAT;
2. Возникает из-за необходимости постоянно поддерживать соединение в активном режиме, но сервер не может “достучаться” до клиента из-за NAT;
3. Можно использовать постоянный “белый” IP адрес, либо использовать пассивный режим, не требующий постоянного соединения.