Практическая работа №12

Сетевая безопасность

Для выполнения данной практической работы необходимо подключиться к лабораторному стенду. Адреса для подключения и пароль выдаст преподаватель во время пары.

Для подключения необходимо использовать VNC-клиент. Скачать его можно на сайте: https://www.realvnc.com/en/connect/download/viewer/ Необходимо выбрать вариант **«Standalone EXE x64»**, и нажать на кнопку «Download VNC Viewer» (рисунок 1).

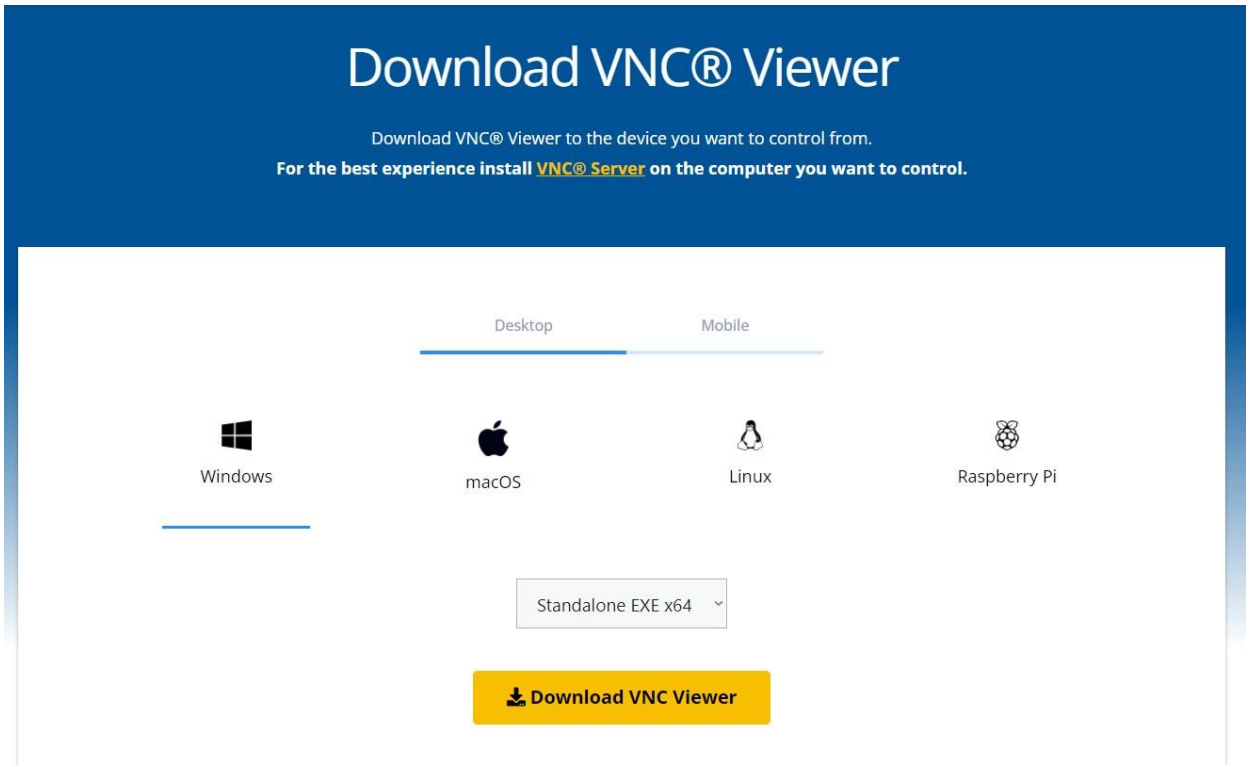

Рисунок 1. Скачивание VNC клиента

Очень многие угрозы информационной безопасности реализуются с помощью компьютерных сетей. Правильная настройка сетевых устройств, служб и ПО, работающего с сетью, является совершенно необходимой для устойчивого и безопасного функционирования любой компьютерной системы.

В первую очередь, это касается настройки межсетевого экрана (он же файерволл, он же брандмауэр). Даже на бытовом, домашнем уровне это достаточно важная задача (ботнеты из старых версий популярных домашних роутеров не дадут соврать). Сегодня в большинстве случаев базовые

настройки поставляемого оборудования уже включают в себя общее правило «не пущать ничего вовнутрь» (т.е. все входящие пакеты, не являющиеся частью уже известных соединений, отбрасываются), что даёт минимально-необходимый уровень безопасности для домашнего использования.

Однако, любая более-менее сложная конфигурация требует ручного управления правилами сетевой фильтрации. Сегодня мы попробуем понять основные принципы работы механизма фильтрации пакетов в ОС Linux, которая преимущественно используется в сетевом оборудовании и серверах.

Основным (но не единственным!) средством фильтрации пакетов в ОС Linux является служба iptables (ранее она называлась ipchains, сегодня она постепенно заменяется службой nftables, имеющей, однако прослойку совместимости с iptables).

В данной работе используется 2 ВМ, одна выполняет роль роутера (с ОС Linux), другая – клиента (с ОС Windows 10).

Для начала, в ОС Windows настроим сеть:

IP-адрес: 192.168.0.x (любой, кроме .1 и .255)

Маска подсети: 255.255.255.0

Шлюз: 192.168.0.1

DNS-сервер: 8.8.8.8

Убедимся, что сеть работает (откроем любой сайт в браузере).

Подключимся к роутеру (ВМ с ОС Linux, логин root пароль 12345) и посмотрим текущие настройки сетевого экрана командой `iptables-save`.

Там должно быть всего 2 правила, необходимые для работы роутером.

Добавим немного фильтрации, например, запретим работать с сайтом vk.com

Для этого нам сначала нужно узнать IP-адрес сайта, поскольку фильтрация работает только с IP-адресами.

```
nslookup vk.com
```

после этого дадим команду на блокировку всех выведенных ip-адресов по очереди

```
iptables -t filter –A FORWARD -d {IP-адрес} -j REJECT --reject-with icmp-host-prohibited
```

Убедимся, что сайт не открывается и не пингуется на ВМ с ОС Windows. Вообще, обычно, для запрета взаимодействия с каким-либо сервисом, особенно для входящих соединений, применяется цель DROP, а не REJECT.Разница между ними заключается в том, что в случае REJECT отправителюзапроса высылается уведомление о невозможности соединения, в случаеDROP запрос просто выбрасывается из очереди обработки, создаваявпечатление, что сайт не работает. Выполним блокировку сервиса mail.ru с целью DROP.

```
nslookup mail.ru
```

```
iptables -t filter -A FORWARD -d {IP-адрес} -j DROP
```

Убедимся, что сайт не открывается и не пингуется на ВМ с ОС Windows. Обратите внимание, что сообщения об ошибках отличаются с предыдущим случаем (зависит от используемого браузера).

Помимо просто фильтрации, сетевой экран позволяет активно вмешиваться в заголовки пакетов. Пример такого вмешательства вы уже знаете — это цель MASQUERADE, используемая для подмены IP-адреса источника.

Помимо настроек сетевых экранов, для обеспечения безопасности требуется также аудит (регулярная проверка). Выполним сканирование нашей сети утилитой nmap (ОС Linux)

```
nmap 192.168.0.0/24
```

Утилита покажет задействованные в подсети IP-адреса и запущенные на этих адресах сервисы.

Для сетевой диагностики также полезным бывает «послушать», какие именно данные идут через соединение. Для этого используется специальное ПО, называемое снифферами.

Стандартным сниффером для ОС Linux является tcpdump.

Запустим эту утилиту командой

```
tcpdump -vv -i enp2s0
```

И откроем какой-нибудь сайт в ОС Windows.

На экране будут представлены заголовки пакетов с пояснениями (опция -vv)

Теперь же сейчас проэкспериментируем с полем TTL. Оно отвечает за количество узлов, которые пакет пройдет, прежде чем будет уничтожен (это необходимо для предотвращения закольцовывания пакетов в случае неправильных таблиц маршрутизации). С помощью этого поля можно выполнять исследование сетей, отправляя пакеты с увеличивающимся значением TTL. Для такого исследования служит утилита tracert.

Определим маршрут до ya.ru (в ОС Windows)

```
tracert ya.ru
```

Теперь изменим это поле в сетевом экране для всех IP-адресов ya.ru (ОС Astra Linux), узнать все адреса через nslookup

```
iptables -t mangle -A PREROUTING -d {IP-адрес} -j TTL --ttl-inc 5
```

Обратите внимание, что в данном случае используется таблица MANGLE (модификация большинства полей заголовков пакетов разрешена только в ней). Повторим команду (в ОС Windows)

```
tracert ya.ru
```

Сравните результат. Данное поле часто используется сотовыми операторами для определения факта «раздачи» интернета мобильными устройствами. Подобное правило на 3G/4G роутере позволяет «обмануть» сотового оператора и использовать телефонные тарифы для работы с сетью.

Заполните файл отчета «Шаблон для практической 12». Прикрепите его в СДО с названием «ПР12_Фамилия_Группа», где в названии будет указана ваша фамилия и группа.

Данный отчет должен содержать скриншоты выполнения работы (замените скриншотом слово <..скриншот..> в соответствующем пункте).

На **ВСЕХ** скриншотах, которые вы делаете, должно быть видно ваше ФИО и группу (для этого откройте блокнот и запишите их там), текущую дату и время и номер ВМ.

Вопросы для самоконтроля

1) Какие еще средства фильтрации есть в ОС LINUX кроме iptables? Укажите преимущества и недостатки других способов фильтрации.

2) Какие могут возникнуть проблемы при неправильной настройке межсетевого экрана?

3) Почему показывается разный результат после первого и второго tracert для ya.ru ?