Практическая работа №13

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).

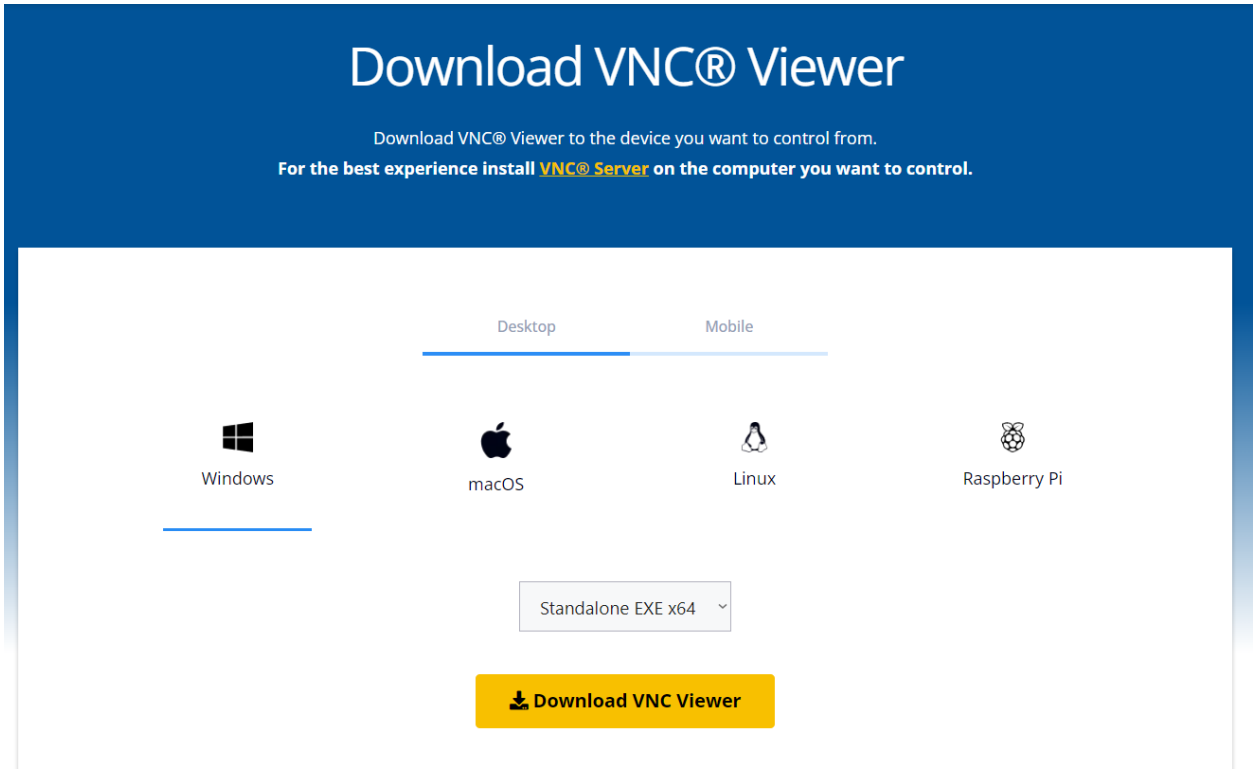

Рисунок 1. Скачивание VNC клиента

Настройка служб гипертекста

Изначально гипертекст был одной из основных частей глобальной сети Интернет. В неё входили и другие службы — электронной почты, новости, мессенджеры. По мере развития сети, все больше и больше сервисов стали обзаводиться гипертекстовыми версиями (многие из вас используют специализированные клиенты электронной почты?), другие же стали использовать гипертекст как транспорт. Сегодня через службы (серверы)

гипертекста реализуется более 90% функциональности глобальной сети (по объёму данных).

Одной из самых популярных реализаций HTTP-сервера является веб-сервер Apache. Он довольно часто используется и в реальных установках (вместе с сервером nGinx), а также входит во всевозможные комплекты «для начинающих». (классический комплект — Apache, MariaDB, PHP, phpmyadmin — для работы с языком PHP)

Установим и настроим веб-сервер apache в среде Astra Linux.

ВНИМАНИЕ! Установка ПО и редактирование глобальной конфигурации осуществляется только **от имени суперпользователя**!

```
apt update
apt install apache2
```

После этого, в принципе, следует проверить работоспособность сервера командой

```
systemctl start apache2
```

и подключившись к нему браузером (для этого необходимо в адресную строку ввести адрес: 127.0.0.1)

Однако, в современной сети работа веб-серверов без шифрования категорически не приветствуется. Поэтому настроим шифрование в установленном экземпляре веб-сервера.

Для начала, следует включить модуль шифрования, поставляемый вместе с веб-сервером apache. В Astra linux для этого выполняем команду

```
ln -s ../mods-available/ssl.load /etc/apache2/mods-enabled/
```

Теперь необходимо внести правки в основной конфигурационный файл сервера.

Открываем файл на редактирование командой

```
nano /etc/apache2/apache2.conf
```

и вставляем в **КОНЕЦ** файла следующие строки

```
<VirtualHost _default_:443>
  ServerName admins.say.mooo.com
  DocumentRoot /var/www/html
  SSLEngine On
  SSLCertificateFile /etc/apache2/ssl/cert.pem
  SSLCertificateKeyFile /etc/apache2/ssl/key.pem
</VirtualHost>
```

При настройке собственного сервера вам необходимо было бы получить подписанный сертификат и приватный ключ самостоятельно (например, через сервис Let's Encrypt), в данном случае сертификат и ключ предоставлены командой поддержки, и находятся в файлах /etc/apache2/ssl/cert.pem и /etc/apache2/ssl/key.pem соответственно.

Для применения конфигурации веб-сервер необходимо перезапустить командой

```
systemctl restart apache2
```

После этого проверьте работоспособность веб-сервера, загрузив на **ОСНОВНОЙ** (не виртуальной!) машине сайт

https://admins.say.mooo.com:91xx для машин группы А

https://admins.say.mooo.com:92xx для машин группы В

где xx — номер вашей виртуальной машины.

Должна открыться страничка приветствия сервера Apache, без ошибок сертификатов (замочек в адресной строке должен указывать наличие шифрования).

Заполните файл отчета «Шаблон для практической 13». Прикрепите его в СДО с названием «ПР13_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.

Не забудьте выключить виртуальную машину после себя (Пуск – Завершение работы).

Вопросы для самоконтроля:

1) В чем преимущества apache перед nginx? В каких ситуациях лучше использовать Apache, а в каких nginx?