Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «КубГУ»)

Факультет компьютерных технологий и прикладной математики

Кафедра информационных технологий

ОТЧЕТ

О выполнении лабораторной работы № 5

По дисциплине «Администрирование в Linux»

Выполнил: ст. гр. 4ИТ/2

Хижний Евгений

Проверил: преподаватель КИТ Прутский А.С.

Краснодар

2021

Лабораторная работа №5.

Цель: поднять виртуальную машину с RDP, FTP, Samba и подключиться к ней при помощи ППО с хост-системы.

Выполнение работы:

**Поднятие RDP**

Для выполнения данной задачи будем использовать **xRDP** — это бесплатная реализация RDP (протокола удаленного рабочего стола) Microsoft с открытым исходным кодом, которая позволяет операционным системам, отличным от Microsoft Windows (таким как Linux и BSD), предоставлять полностью функциональный RDP-совместимый удаленный рабочий стол и **Xfce** — свободная среда рабочего стола для UNIX-подобных операционных систем, таких, как GNU/Linux, NetBSD, OpenBSD, FreeBSD, Solaris и т. п. Конфигурация данной среды полностью управляется мышью, конфигурационные файлы скрыты от пользователя. Xfce основана на GTK+ и использует собственный менеджер окон Xfwm.

Для этого выполняем следующие команды в терминале:

**sudo apt-get install xrdp**

**sudo apt-get install xfce4**

**sudo systemctl enable xrdp**

**sudo ufw allow from [ip]/24 to any port 3389**

s**udo service xrdp restart**

**Для подключения из хост-системы(Windows) переходим в командную строку и пишем mstsc /v:[ip]. Откроется окно для ввода логина и пароля для подключения**

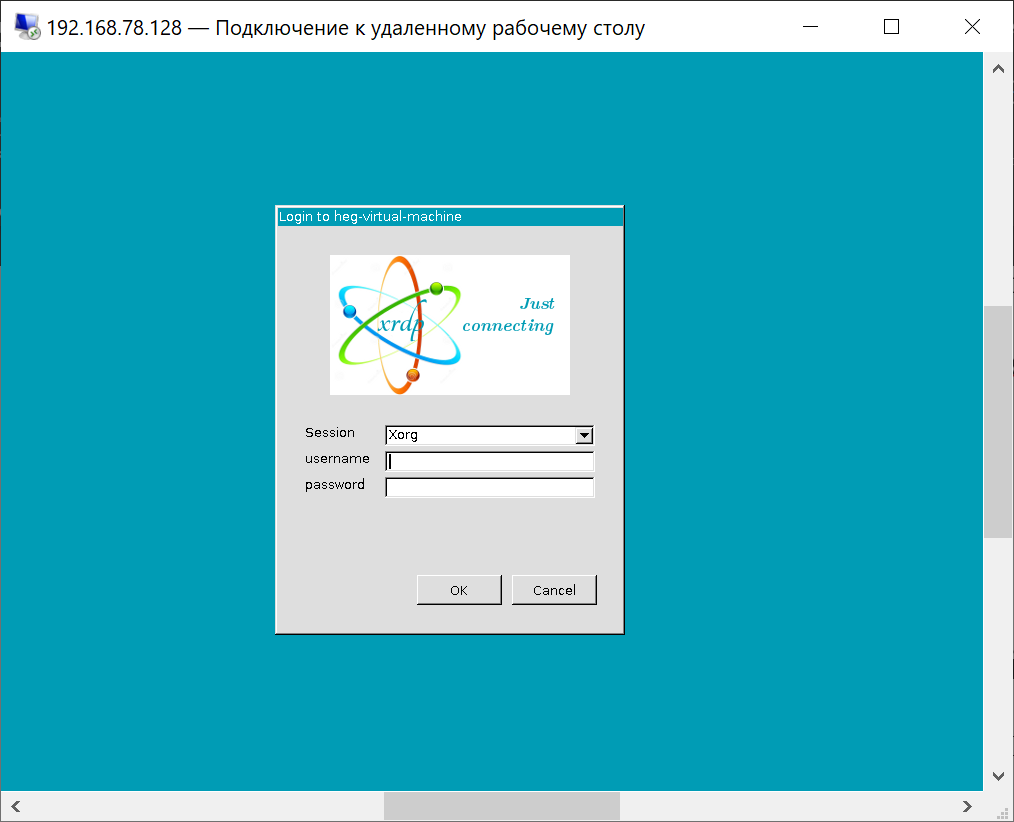


Рисунок 1 — окно ввода пароля

После ввода пароля мы получаем доступ к нашей виртуальной машине при помощи RDP в Windows.



Рисунок 2— удаленный рабочий стол

**Поднятие FTP**

Для выполнения данной задачи будем устанавливать **vsftpd** (Very Secure Ftp Daemon), стабильный, безопасный и быстрый FTP-сервер.

Для это выполним следующие команды:

sudo apt update

sudo apt install vsftpd

Служба ftp автоматически запустится после завершения процесса установки. Чтобы проверить это, распечатаем статус службы:

sudo systemctl status vsftpd

sftpd.service - vsftpd FTP server

Вывод должен показать, что служба vsftpd активна и работает:

Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)

Active: active (running) since Tue 2021-11-02 19:19:25 +03; 4min 24s ago

**Настройка vsftpd:**

откроем файл конфигурации vsftpd:

sudo nano /etc/vsftpd.conf

Вставим следующие поля:

listen=NO

listen\_ipv6=YES

anonymous\_enable=NO

local\_enable=YES

write\_enable=YES

dirmessage\_enable=YES

use\_localtime=YES

xferlog\_enable=YES

connect\_from\_port\_20=YES

chroot\_local\_user=YES

secure\_chroot\_dir=/var/run/vsftpd/empty

pam\_service\_name=vsftpd

user\_sub\_token=$USER

local\_root=/home/$USER/ftp

pasv\_min\_port=30000

pasv\_max\_port=31000

userlist\_enable=YES

userlist\_file=/etc/vsftpd.user\_list

userlist\_deny=NO

Чтобы зашифровать передачи FTP с помощью SSL / TLS, потребуется сертификат SSL и настроить FTP-сервер для его использования.

Сгенерируем 2048-битный закрытый ключ и самозаверяющий SSL-сертификат, который будет действителен в течение десяти лет:

sudo openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

После этого добавиv в файл конфигурации vsftpd:

rsa\_cert\_file=/etc/ssl/private/vsftpd.pem

rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem

ssl\_enable=YES

Сохраним файл и перезапустим службу vsftpd, чтобы изменения вступили в силу:

sudo systemctl restart vsftpd

**Открытие брандмаузера:**

Чтобы открыть порт 21 (командный порт FTP), порт 20 (порт данных FTP) и 30000–31000 (диапазон пассивных портов), выполните следующие команды:

sudo ufw allow 20:21/tcp

sudo ufw allow 30000:31000/tcp

Чтобы избежать блокировки, убедитесь, что порт 22 открыт:

sudo ufw allow OpenSSH

Перезагрузим правила UFW, отключив и снова включив UFW:

sudo ufw disable

sudo ufw enable

Чтобы проверить изменения, выполним:

sudo ufw status

Status: active

To Action From

-- ------ ----

20:21/tcp ALLOW Anywhere

30000:31000/tcp ALLOW Anywhere

OpenSSH ALLOW Anywhere

20:21/tcp (v6) ALLOW Anywhere (v6)

30000:31000/tcp (v6) ALLOW Anywhere (v6)

OpenSSH (v6) ALLOW Anywhere (v6)

**Создаение пользователя FTP:**

Создадим нового пользователя с именем newftp:

sudo adduser newftp

Добавим пользователя в список разрешенных пользователей FTP:

echo "newftp" | sudo tee -a /etc/vsftpd.user\_list

Создадим дерево каталогов FTP и установите правильные разрешения:

sudo mkdir -p /home/newftp/ftp/upload

sudo chmod 550 /home/newftp/ftp

sudo chmod 750 /home/newftp/ftp/upload

sudo chown -R newftp: /home/newftp/ftp

На этом ftp-сервер работает, попробуем подключится к нему с хоста.

Для этого будем использовать встроенные возможности windows.

Нажмем правой кнопкой мыши на «Этот компьютер»-> «Добавить новый элемент в сетевое окрудение», нажимаем «Далее», «Далее», вводим ftp-адрес: ftp://[ip], нажимаем «Далее», убираем галочку с «Анонимный вход», в поле «Пользователь вводим «newftp», нажимаем «Далее», вводим имя для данного подключения: «ftptest», нажимаем «Далее», нажимаем «Готово». Нажимаем на созданное подлкючение, вводим пароль. Мы должны иметь доступ к папке upload.

На этом задача выполнена.

Изображение выглядит как текст, снимок экрана, монитор, экран

Автоматически созданное описание

Рисунок 3 — папка upload на ftp-сервере

**Поднятие Samba**

По умолчанию, в системах на базе Debian брандмауэр разрешает все соединения. Но если в нашем случае мы используем брандмауэр, необходимо открыть порты:

sudo iptables -I INPUT -p tcp --dport 445 -j ACCEPT

sudo iptables -I INPUT -p udp --dport 137:138 -j ACCEPT

sudo iptables -I INPUT -p tcp --dport 139 -j ACCEPT

Применяем настройки:

sudo apt-get install iptables-persistent

sudo netfilter-persistent save

Установка Samba выполняется из репозитория одной командой:

sudo apt-get install samba

Проверим, что сервис запустился:

sudo systemctl status smbd

Создадим две папки и предоставим им права доступа:

mkdir -p /data/public

chmod 777 /data/public

mkdir /data/private

chmod 777 /data/private

И добавляем настройки для папок:

sudo nano /etc/samba/smb.conf

[public]

comment = Public Folder

path = /data/public

public = yes

writable = yes

read only = no

guest ok = yes

create mask = 0777

directory mask = 0777

force create mode = 0777

force directory mode = 0777

[private]

comment = Private Folder

path = /data/private

public = no

writable = yes

read only = no

guest ok = no

create mask = 0777

directory mask = 0777

force create mode = 0777

force directory mode = 0777

Теперь создадим пользователя в samba:

smbpasswd -a heg

Перезапускаем samba:

systemctl restart smbd

Настройка завершена, переходим в windows.

Открываем проводник, переходив во вкладку «Сеть», и в строке пишем «\\[ip\_ubuntu]», вводим логин и пароль для пользователя samba и получаем доступ к папкам на сервере.

Изображение выглядит как текст, снимок экрана, монитор, экран

Автоматически созданное описание

Рисунок 4 — папки на samba-сервере

Таким образом поставленная цель выполнена.