

Отчёт по прохождению внешнего курса: Системный администратор Linux с нуля

Часть 3

Анастасия Мазуркевич

Содержание

1 Цель работы	4
2 Ход выполнения	5
2.1 Основы сетевой конфигурации в Linux	5
2.2 Базовая диагностика сети	8
2.3 Настройка SSH-доступа и его защита	11
2.4 Повышение безопасности сетевого взаимодействия	16
2.5 модуль 9	19
3 Заключение	21

Список иллюстраций

2.1 скрин задания	5
2.2 скрин задания	6
2.3 скрин задания	7
2.4 скрин задания	7
2.5 скрин задания	8
2.6 скрин задания	9
2.7 скрин задания	9
2.8 скрин задания	10
2.9 скрин задания	11
2.10 скрин задания	12
2.11 скрин задания	12
2.12 скрин задания	13
2.13 логи ssh	14
2.14 скрин вопроса	15
2.15 скрин вопроса	16
2.16 скрин вопроса	16
2.17 скрин вопроса	17
2.18 скрин вопроса	17
2.19 скрин вопроса	18
2.20 скрин вопроса	19
2.21 скрин вопроса	19
2.22 скрин вопроса	20

1 Цель работы

Изучить основы системного администрирования и Linux

2 Ход выполнения

2.1 Основы сетевой конфигурации в Linux

Какой командой можно назначить IP-адрес вручную? ip a add 192.168.122.2/24 dev eth0

Тест по теме «Основы сетевой конфигурации в Linux»

Какой командой можно назначить IP-адрес вручную?

ip a add 192.168.122.2/24 dev eth0

ip set eth0 192.168.122.2

ip config dev eth0 address 192.168.122.2

ip add dev eth0 192.168.122.2

1/5

Рис. 2.1: скрин задания

Что делает директива auto eth0 в /etc/network/interfaces? Верный ответ: Поднимает интерфейс автоматически при загрузке системы

Тест по теме «Основы сетевой конфигурации в Linux»

Что делает директива auto eth0 в /etc/network/interfaces?

- Поднимает интерфейс автоматически при загрузке системы
- Запускает dhclient при подключении интерфейса
- Назначает статический IP при старте
- Настраивает интерфейс при появлении линка

2/

Рис. 2.2: скрин задания

Какая команда используется для удаления IP с интерфейса? Верный ответ: ip a
del 192.168.122.2/24 dev eth0

Тест по теме «Основы сетевой конфигурации в Linux»

Какая команда используется для удаления IP с интерфейса?

ip del addr 192.168.122.2 dev eth0

ip a del 192.168.122.2/24 dev eth0

ip addr flush dev eth0

ip a down 192.168.122.2 dev eth0

3/5

Рис. 2.3: скрин задания

Что произойдет при перезагрузке, если IP-адрес был задан только через ip?

Верный ответ: IP-адрес исчезнет

Тест по теме «Основы сетевой конфигурации в Linux»

Что произойдет при перезагрузке, если IP-адрес был задан только через ip?

IP-адрес будет автоматически восстановлен

Настройка сохранится в /etc/network/interfaces

IP-адрес исчезнет

Система создаст интерфейс заново

4/5

Рис. 2.4: скрин задания

Где задается шлюз по умолчанию в конфигурации интерфейса? Верный ответ:
В поле gateway в /etc/network/interfaces

Тест по теме «Основы сетевой конфигурации в Linux»

Где задается шлюз по умолчанию в конфигурации интерфейса?

В настройках DNS-сервера

В поле gateway в /etc/network/interfaces

В resolv.conf

В /etc/hosts

5/5

Рис. 2.5: скрин задания

2.2 Базовая диагностика сети

Какая команда показывает открытые TCP-порты и процессы, которые их слушают? Верный ответ: ss -tulnp

Тест по теме «Базовая диагностика сети»

Какая команда показывает открытые TCP-порты и процессы, ко

- netstat -an
- ping
- ss -tulnp
- nc -l

1/4

Рис. 2.6: скрин задания

Какой флаг в ss включает отображение номеров портов и PID/имен процессов?

Верный ответ: -r

Тест по теме «Базовая диагностика сети»

Какой флаг в ss включает отображение номеров портов и PID/имен

- n
- l
- p
- t

2/4

Рис. 2.7: скрин задания

Что делает команда dig? Верный ответ: Выполняет DNS-запрос и отображает IP-адреса

Тест по теме «Базовая диагностика сети»

Что делает команда dig?

- Определяет местоположение хоста
- Диагностирует сетевые маршруты
- Отправляет эхо-запросы
- Выполняет DNS-запрос и отображает IP-адреса

3/4

Рис. 2.8: скрин задания

Какая команда может использоваться для проверки подключения к удаленному TCP-порту без передачи данных? Верный ответ: nc -vz

Тест по теме «Базовая диагностика сети»

Какая команда может использоваться для проверки подключения порту без передачи данных?

nc -vz

curl

scp

wget

4/4

Рис. 2.9: скрин задания

2.3 Настройка SSH-доступа и его защита

Какой порт использует SSH по умолчанию? Верный ответ: 22

Тест по теме «Настройка SSH-доступа и его защита»

Какой порт использует SSH по умолчанию?

20

443

22

21

1/5

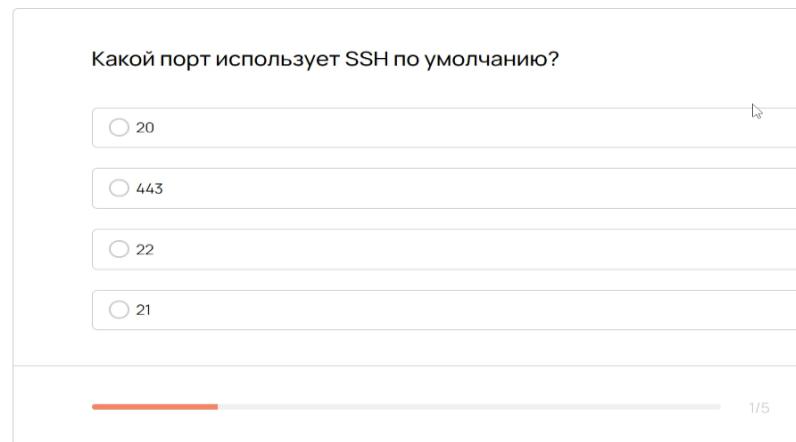


Рис. 2.10: скрин задания

Где находится основной конфигурационный файл демона SSH-сервера? Верный ответ: /etc/ssh/sshd_config

Тест по теме «Настройка SSH-доступа и его защита»

Где находится основной конфигурационный файл демона SSH-сервера?

/etc/hosts

/etc/ssh/sshd_config

~/.ssh/config

/etc/ssh/sshd_config

2/5

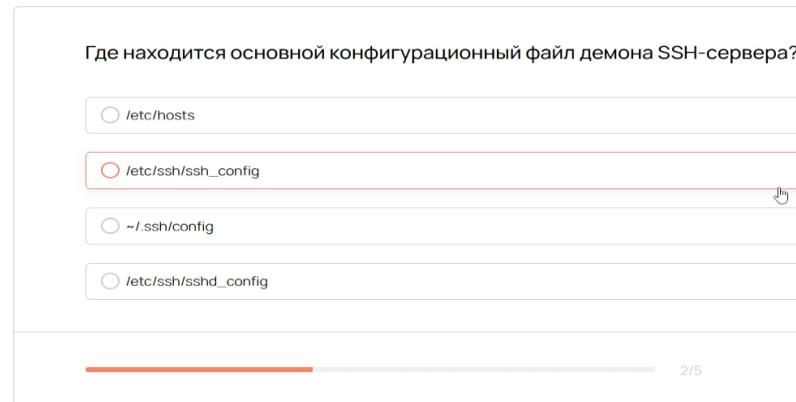


Рис. 2.11: скрин задания

Какой командой можно временно остановить службу SSH (systemd)? Верный ответ: systemctl stop ssh

Тест по теме «Настройка SSH-доступа и его защиты»

Какой командой можно временно остановить службу SSH (systemd)?

killall sshd

service ssh restart

systemctl disable ssh

systemctl stop ssh

3/5



Рис. 2.12: скрин задания

Какой файл публичного ключа нужно добавить на сервер для авторизации по ключу? Верный ответ: id_rsa.pub

Тест по теме «Настройка SSH-доступа и его защита»

Какой файл публичного ключа нужно добавить на сервер для авторизации

id_rsa.pub

authorized_keys

known_hosts

id_rsa

 4/5

Рис. 2.13: логи ssh

Какой параметр в sshd_config отключает вход пользователя root по SSH? Верный ответ: PermitRootLogin no

Тест по теме «Настройка SSH-доступа и его защиты»

Какой параметр в sshd_config отключает вход пользователя root по

Port 2222

PermitRootLogin no

PasswordAuthentication no

AllowUsers root

 5/5

 3

Рис. 2.14: скрин вопроса

2.4 Повышение безопасности сетевого взаимодействия

Тест по теме «Повышение безопасности сетевого взаимодействия»

Какой командой включить (activate) файрвол UFW?

ufw start

ufw enable

systemctl start ufw

service ufw on

1/5

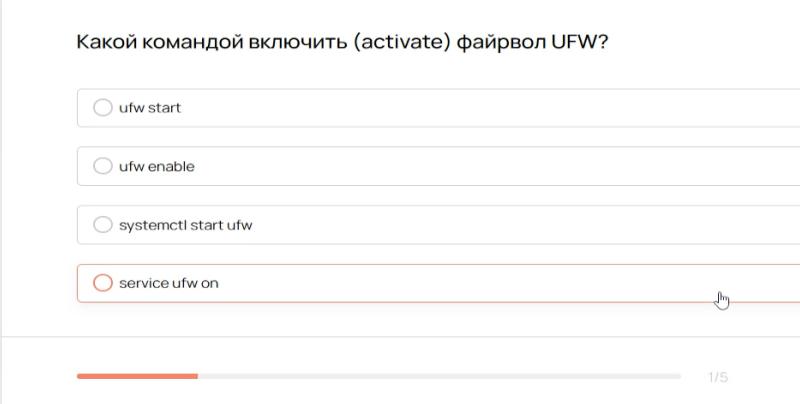


Рис. 2.15: скрин вопроса

Тест по теме «Повышение безопасности сетевого взаимодействия»

В каком файле fail2ban хранит свои jail-конфигурации по умолчанию?

/etc/fail2ban/fail2ban.conf

/etc/fail2ban/jail.conf

/etc/fail2ban/jail.local

/etc/fail2ban/filters/jail.conf

2/5



Рис. 2.16: скрин вопроса

Тест по теме «Повышение безопасности сетевого взаимодействия»

Какой флаг UFW позволяет указать конкретный номер правила для удаления

--remove
 --delete
 --num
 --dry-run

3/5

Рис. 2.17: скрин вопроса

Тест по теме «Повышение безопасности сетевого взаимодействия»

Какой параметр в jail-файле fail2ban задает время блокировки IP в секундах

maxretry
 bantime
 findtime
 backend

4/5

Рис. 2.18: скрин вопроса

Тест по теме «Повышение безопасности сетевого взаимодействия»

Какая команда добавит в UFW разрешение на SSH (порт 22) только 192.168.1.0/24?

- ufw allow 22
- ufw allow from 192.168.1.0/24 to any port 22
- ufw allow in 192.168.1.0/24 22
- ufw allow 22/tcp 192.168.1.0/24

5/5

Рис. 2.19: скрин вопроса

2.5 модуль 9

Тест по теме «Что такое пакеты и как они устроены»

Какую команду нужно выполнять регулярно?

apt update

man sources.list

apt show

apt install

— 3/3

Завершить

Рис. 2.20: скрин вопроса

Тест по теме «Что такое пакеты и как они устроены»

Если нужно удалить пакет и его зависимости, оставив только конфигурационные файлы, какую команду будете использовать?

purge

depends

remove

autoremove

— 1/3

Рис. 2.21: скрин вопроса

Тест по теме «Что такое пакеты и как они устроены»

Какую команду нужно использовать, чтобы удалить пакет и конфигурацию оставить зависимости?

delete

autopurge

remove

purge

2/3

Рис. 2.22: скрин вопроса

3 Заключение

Освоили основы администрирования по внешнему курсу Linux с yekz