

Внешний курс. Часть 3

Аджигалиева Амина Руслановна

20 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

Изучить основы системного администрирования и Linux

Освоение сетевых технологий, безопасности и контейнеризации

Основы сетевой конфигурации

ip a add 192.168.122.2/24 dev eth0 - ручное назначение IP

Тест по теме «Основы сетевой конфигурации в Linux»

Какой командой можно назначить IP-адрес вручную?

ip config dev eth0 address 192.168.122.2

ip a add 192.168.122.2/24 dev eth0

ip add dev eth0 192.168.122.2

Автозапуск интерфейса

auto eth0 - поднимает интерфейс при загрузке

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

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

Рис. 2: Автозапуск интерфейса

Удаление IP-адреса

ip a del 192.168.122.2/24 dev eth0 - удаление IP

Какая команда используется для удаления IP с интерфейса?

ip a down 192.168.122.2 dev eth0

ip del addr 192.168.122.2 dev eth0

ip a del 192.168.122.2/24 dev eth0

ip addr flush dev eth0

Рис. 3: Удаление IP

Сетевая диагностика

Просмотр открытых портов

`ss -tulnp` - показывает TCP-порты и процессы

Тест по теме «Базовая диагностика сети»

Какая команда показывает открытые TCP-порты и процессы, которые их слушают?

netstat -an

ping

ss -tulnp

nc -l

Рис. 4: Команда ss

`dig` - выполнение DNS-запросов

Что делает команда `dig`?

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



Рис. 5: Команда `dig`

Проверка портов

`nc -vz` - проверка TCP-подключения

Какая команда может использоваться для проверки подключения к удаленному TCP-порту без передачи данных?

nc -vz



curl

scp

wget

Рис. 6: Команда nc

Безопасность SSH

22 - стандартный порт SSH

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

Какой порт использует SSH по умолчанию?

21

22

20

Конфигурация SSH

/etc/ssh/sshd_config - основной конфиг файл

Где находится основной конфигурационный файл демона SSH-сервера?

~/.ssh/config

/etc/hosts

/etc/ssh/sshd_config

/etc/ssh/sshd_config

Рис. 8: Конфиг SSH

Остановка SSH-сервиса

`systemctl stop ssh` - временная остановка

Какой командой можно временно остановить службу SSH (systemd)?

killall sshd

service ssh restart

systemctl stop ssh



systemctl disable ssh

Рис. 9: Остановка SSH

Управление пакетами

Изучение устройства пакетов в Linux

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?

remove

autoremove

purge

depends

Команды для обновления пакетов

Тест по теме «Обновление системы и безопасность»

С помощью какого пакета можно настроить автоматическое обновление системы?

htop

gzip

update

unattended-upgrades

Рис. 11: Обновление системы

Решение конфликтов пакетов

Тест по теме « Работа с зависимостями и решение конфликтов»

Что случится, если вы удалите какой-то пакет, от которого зависимы другие пакеты?

Сервер выключится

Сработает apt-cache search

Разрыв зависимостей

Рис. 12: Зависимости пакетов

Работа с логами

Изучение системы логов в Linux

Тест по теме «Знакомство с логами»

Какие три ключевые задачи системного администратора решаются с помощью анализа логов, согласно материалу урока?

- Установка обновлений, настройка сети, резервное копирование
- Диагностика сбоев, расследование инцидентов безопасности, аудит производительности
- Управление пользователями, настройка файрвола, мониторинг дискового пространства
- Компиляция ядра, написание скриптов, управление пакетами

Рис. 13: Основы логирования

Работа с системными логами

Тест по теме «Система логирования в Linux»

Каково типичное взаимодействие между systemd-journald и rsyslog в современных дистрибутивах Linux?

- rsyslog собирает все логи и передает их в systemd-journald
- systemd-journald и rsyslog работают полностью независимо и не взаимодействуют
- systemd-journald собирает все системные сообщения и может перенаправлять их в rsyslog для записи в текстовые файлы
- rsyslog является устаревшей технологией и полностью заменен на systemd-journald

Рис. 14: Система логов

Поиск и фильтрация лог-записей

Тест по теме «Поиск и фильтрация логов под конкретные задачи»

У вас есть файл с IP-адресами, многие из которых повторяются. Какой конвейер команд правильно подсчитает количество вхождений каждого уникального IP-адреса?

uniq -c | sort -nr ip_list.txt

sort ip_list.txt | uniq -c

uniq ip_list.txt | sort

awk '{print \$1}' ip_list.txt | uniq

Расследование инцидентов

Исследование инцидентов безопасности

Тест по теме «Расследование инцидентов по логам»

Вы наблюдаете в логах сотни попыток входа за короткое время для пользователей admin, root, test, user с одного и того же IP-адреса. Какой тип активности это, скорее всего, означает?

- Системный сбой, вызвавший повторные попытки подключения
- Пользователь, который забыл свой логин и пароль
- Автоматизированная атака по подбору пароля (brute-force) и перебору имен пользователей
- Нормальная активность службы мониторинга

Управление жизненным циклом лог-файлов

Какую основную и наиболее насущную проблему решает утилита logrotate?

- Анализ логов на предмет угроз безопасности
- Централизованный сбор логов с нескольких серверов
- Предотвращение исчерпания свободного места на диске из-за неконтролируемого роста лог-файлов
- Уведомление администратора об ошибках в реальном времени

Рис. 17: Ротация логов

Контейнеризация

Изучение принципов контейнеризации

Тест по теме «Контейнеризация как подход»

Какая команда позволяет проверить конфигурацию Podman?

podman run --check

podman system

podman info

podman status

Управление контейнерами в Podman

Тест по теме «Работа с контейнерами в Podman»

Какая команда запускает контейнер с пробросом порта 8080 на 80?

podman expose 8080:80 nginx

podman publish -p 8080:80 nginx

podman run -p 8080:80 nginx

podman exec -p 8080:80 nginx

Контроль ресурсов контейнеров

Тест по теме «Управление ресурсами контейнеров»

Какая команда позволяет отслеживать использование ресурсов контейнера в реальном времени?

podman list

podman run

podman ps

podman stats

Безопасность контейнеров

Работа с Docker-образами

Тест по теме «Образы, реестры и базовая безопасность»

Какая команда используется для загрузки образа из реестра?

podman fetch

podman load

podman clone

podman pull

Основы безопасной работы с контейнерами

Где хранится политика доверия для Podman?

- /etc/pki/policy.json
- /usr/share/podman/trust
- /etc/containers/policy.json
- /etc/podman/trust.json

Результаты обучения

Все тесты курса пройдены успешно

Тест по теме «Образы, реестры и базовая безопасность»

Результат тестирования

Тест пройден

4 из 4

Итоги курса

- Освоены основы сетевой конфигурации
- Изучена диагностика сети
- Приобретены навыки безопасности SSH
- Освоено управление пакетами
- Изучена работа с системными логами
- Освоены основы контейнеризации