ПРАКТИЧЕСКОЕ ЗАДАНИЕ 3.7
Тема: ОС Linux: установка, настройка и обеспечение информационной безопасности

УЧЕБНЫЕ ВОПРОСЫ

1. Установка и базовая настройка ОС Linux.
2. Общий аудит безопасности в Linux.
3. Анализ уязвимостей системы.
4. Сетевой мониторинг и контроль активности.

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

- **Установка Linux**: выбор дистрибутива, разметка диска, настройка пользователей и сети, обновление системы.
- **Аудит безопасности**: проверка журналов (/var/log/), пользователей и прав, активных сервисов, сетевых соединений.
- **Анализ уязвимостей**: использование lynis, chkrootkit, rkhunter, nmap.
- **Сетевой мониторинг**: iftop, tcpdump, wireshark.

1. Установка и настройка Linux

Linux — свободная ОС с открытым исходным кодом. Популярные дистрибутивы: Ubuntu, Debian, CentOS, Fedora.
Этапы установки:

1. Выбор дистрибутива (например, Ubuntu — для новичков, Debian — для стабильности, CentOS — для серверов).
2. Настройка разделов диска (обычно: /, /home, swap).
3. Создание учетной записи пользователя.
4. Настройка сети (DHCP или статический IP).
5. Обновление системы после установки:
6. sudo apt update && sudo apt upgrade # для Debian/Ubuntu
7. sudo dnf update # для Fedora

✅ Зачем: обновления устраняют уязвимости и повышают стабильность.

---

2. Общий аудит безопасности

Журналы системы

- /var/log/syslog — общий системный журнал.
- /var/log/auth.log — события входа в систему и sudo.

Примеры:
sudo tail -n 20 /var/log/syslog
👉 показывает последние 20 строк системного журнала.
Используется для поиска ошибок сервисов и состояния системы.
sudo grep "Failed password" /var/log/auth.log
👉 выводит неудачные попытки входа. Это помогает выявить перебор паролей (bruteforce).

Проверка пользователей и прав

cat /etc/passwd

👉 список всех учетных записей.

Если встречаются необычные пользователи с /bin/bash в конце — стоит проверить, кто их создал.

id username

👉 показывает UID, GID и группы конкретного пользователя.

Активные сервисы

systemctl list-units --type=service

👉 список запущенных служб. Например, если видим открытую службу telnet, это угроза безопасности.

Сетевые соединения

ss -tulpn

👉 список процессов, слушающих порты. Можно сразу понять, какие сервисы доступны извне.

---

3. Анализ уязвимостей

Lynis

Инструмент для комплексного аудита.

sudo lynis audit system

👉 программа проверит десятки параметров: от конфигурации ядра до SSH.

Результат: индекс безопасности + рекомендации.

Пример: *«Disable root login via SSH»* — значит, надо запретить вход root по SSH.

chkrootkit и rkhunter

Инструменты для поиска руткитов (вредоносных программ, скрывающихся в системе).

sudo chkrootkit

sudo rkhunter --check

👉 проверяют наличие подозрительных файлов, процессов и изменений в системе.

Применяются при подозрении на взлом.

nmap

Сканер сетевых портов.

nmap -sV 192.168.56.101

👉 покажет открытые порты и версии сервисов.

Пример результата:

22/tcp open ssh OpenSSH 8.2

80/tcp open http Apache 2.4.41

Это значит: на машине работает SSH и Apache. Если сервисы не нужны — их нужно закрыть.

---

4. Сетевой мониторинг

iftop

Мониторинг сетевых соединений в реальном времени.

sudo iftop

👉 показывает, кто с кем соединен, сколько трафика передается.
Применяется для поиска подозрительных соединений (например, утечка данных на неизвестный IP).

tcpdump

Анализ сетевых пакетов.
sudo tcpdump port 80
👉 перехватывает трафик по HTTP (порт 80).
Можно увидеть незашифрованные запросы (логины/пароли, если не используется HTTPS).

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие основные этапы установки ОС Linux вы знаете?
2. Какие действия включаются в аудит безопасности Linux?
3. Назовите инструменты анализа уязвимостей в Linux.
4. Как можно выявить незашифрованный сетевой трафик?
5. Для чего используется tcpdump и какую информацию он дает?
6. Чем отличается аудит безопасности от анализа уязвимостей?
7. Какие меры можно предпринять для повышения безопасности ОС Linux после установки?

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. **Установка Linux**
   - Установите дистрибутив (Ubuntu/Debian).
   - Создайте учетную запись пользователя, настройте пароль и обновите систему.
2. **Работа с пользователями**
   - Настройте учетную запись (создание, пароли, группы, оболочка).
   - Проверьте наличие учетных записей без пароля или с UID=0.
   - Составьте список всех пользователей и групп системы.
3. **Системные журналы**
   - Ознакомьтесь с журналами /var/log/syslog и /var/log/auth.log.
   - Зафиксируйте интересные события (например, входы, ошибки, перезапуски сервисов).
4. **Аудит с помощью Lynis**
   - Установите и запустите Lynis: sudo lynis audit system.
   - Зафиксируйте рекомендации программы и сделайте выводы.
5. **Проверка на руткиты**
   - Выполните проверку с помощью chkrootkit или rkhunter.
   - Зафиксируйте результаты (скриншоты и выводы).
6. **Сканирование сети**
   - Проведите сканирование своей VM с помощью nmap.
   - Определите открытые порты и их назначение.
7. **Мониторинг сети**
   - Запустите iftop или tcpdump.

- Проанализируйте активные соединения и сетевую активность.

8. **Отчет**
   - Составьте отчет в MS Word:
     - В начале: номер группы, фамилия, тема («0341 Иванов Linux»).
     - Для каждого задания: описание действий + скриншоты.
     - В конце: ответы на контрольные вопросы.