Лабораторная работа №1

Тема: Базовая защита SSH-сервера и фильтрация трафика в Debian 12

Дисциплина: Системное администрирование

Студент: Чуев Никита Сергеевич

Группа: p4250

Преподаватель: Некрасов Евгений Андреевич

Дата выполнения: 08.09.2025

Цель и задачи

Цель: освоить базовые методы защиты сервера и фильтрации трафика.

Задачи:

- Перенести SSH на порт 22222.
- Создать пользователя и отключить root-доступ.
- Запретить вход по паролю, оставить только ключи.
- Настроить iptables для ограничения доступа.
- Установить Fail2ban.
- Проанализировать логи подключений.
- Добавить приветственное сообщение (MOTD).

Среда клиента: Windows 11 (PuTTYgen, PuTTY).

Используемые технологии

- Сервер: Debian 12 (Bookworm)
- Клиент: Windows 11
- Сетевой доступ: OpenSSH
- Безопасность: iptables, Fail2ban
- Инструменты: PuTTYgen, PuTTY, nmap

Настройка SSH

Изменены параметры в /etc/ssh/sshd_config:

Port 22222
PermitRootLogin no
PasswordAuthentication no

Создан пользователь и выданы права sudo:

adduser nikitachuev
usermod -aG sudo nikitachuev

Перезапуск службы: systemctl restart ssh

Подключение (Windows 11): ssh -p 22222 nikitachuev@192.168.0.108

Настройка iptables

Разрешены loopback и активные соединения; открыты только SSH (22222) и HTTP (80); остальное заблокировано.

Правила:

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --dport 22222 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -j DROP
```

Проверка: nmap -sT localhost → 22222/tcp open ssh, 80/tcp open http

Fail2ban

Установка: apt install fail2ban -y

Принцип: автоблокировка IP после 3–5 неверных попыток.

Фрагмент лога:

2025-09-08 15:22:41 fail2ban.actions [INFO] Ban 192.168.0.111
2025-09-08 15:27:41 fail2ban.actions [INFO] Unban 192.168.0.111

Анализ логов

Просмотр: less /var/log/auth.log

Сводка:

192.168.0.105 — FAILED: 0, OK: 4
192.168.0.109 — FAILED: 0, OK: 1

Вывод: все подключения успешные, неудачных попыток не обнаружено.

Приветственное сообщение (MOTD)

Изменён файл /etc/motd.

При входе отображается системная информация и приветствие.

Фрагмент: IPv4: 192.168.0.108; Load: 10%; Uptime: 29 min; CPU: 39°C; Привет!

Итоги выполнения

- SSH перенесён на порт 22222, root-доступ отключён.
- Создан пользователь nikitachuev; вход только по ключам (Windows 11).
- iptables фильтрует трафик; открыты только нужные порты.
- Fail2ban блокирует подозрительные IP.
- Анализ логов подтвердил корректную работу.
- Настроено приветственное сообщение (MOTD).

Все задачи выполнены успешно.

Благодарю за внимание!