Этапы работы

- Перенос SSH на нестандартный порт
- Создание пользователя и настройка SSH-ключей
- Настройка iptables
- Установка Fail2ban
- Анализ логов
- Добавление приветственного сообщения пользователю

Задание 1 — Настройка SSH

- **Цель:** смена порта, отключение root, разрешить только ключи, создать пользователя с правами sudo.
- **Действия:** изменён `/etc/ssh/sshd_config` (Port 30781, PermitRootLogin no, PasswordAuthentication no), создан `admin`, перезапущен сервис.
- **Ключи:** сгенерированы в PuTTYgen; публичный ключ добавлен в `/home/admin/.ssh/authorized_keys`.
- **Проверка:** подключение к `192.168.0.109:30781` — успешно.

Задание 2 — Настройка iptables

- **Цель:** оставить только loopback, ESTABLISHED, SSH(в данном случае 30781) и HTTP(80), блокировать остальное.
- **Основные команды:**

```
sudo iptables -A INPUT -i lo -j ACCEPT sudo iptables -A
INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 30781 -j ACCEPT sudo
iptables -A INPUT -p tcp --dport 80 -j ACCEPT sudo iptables
-A INPUT -j DROP
```

Задание 3 — Fail2ban

- **Действие:** установка `sudo apt install fail2ban -y`.
- **Настройка:** правило блокировки при 3–5 неверных попытках по умолчанию.
- **Результат:** при грубой атаке IP автоматически блокируется — защита от перебора паролей.

Задание 4 — Логирование и анализ

- **Инструмент:** awk `/var/log/auth.log*` и подсчёта FAILED/OK по IP.
- **Ключевая команда:** bash-скрипт извлекает строки Failed/Accepted, определяет IP и суммирует счётчики посредством awk.
- **Результат:** в выборке отмечен IP `192.168.0.111` (1 FAIL, 5 OK).

Задание 5 — Приветственное сообщение

- **Цель:** отображать при входе приветствие пользователю.
- **Действие:** отредактирован `/etc/motd`, добавлено сообщение: "Velcome to debian experimental server! Have fun!"

Проблемы и замечания

- Существенных проблем не возникло — работа выполнена штатно.

Результаты работы

- SSH работает на порту **30781** и доступен только по ключам.
- Создан пользователь **admin** с правами sudo.
- iptables ограничивает трафик, открыты только необходимые порты.
- Fail2ban установлен и защищает от перебора паролей.
- Проведён анализ логов — подготовлена таблица по IP.
- MOTD отображает системную информацию и приветствие.

Итог

Работа выполнена в полном объёме. Система настроена и защищена.

Заключение

Благодарю за внимание!

Если есть вопросы, я готов на них ответить.

Ковалев Никита