SSH HARDENING + FAIL2BAN

ШАГ 1: СОЗДАТЬ ПОЛЬЗОВАТЕЛЯ

ЗАЧЕМ: Root — слишком мощный. Если хакер войдёт под root → он получит полный контроль.

```
# Создать пользователя sshuser
useradd -m -s /bin/bash sshuser

# Установить пароль
passwd sshuser
```

Введёшь пароль: `P@ssw0rd`

ШАГ 2: НАСТРОИТЬ SSH

ЗАЧЕМ: Запретить вход root, разрешить только sshuser.

```
# Открыть конфиг SSH
nano /etc/ssh/sshd_config
```

НАЙДИ И ИЗМЕНИ:

```
PermitRootLogin no
AllowUsers sshuser
```

Перезапустить SSH:

```
systemctl restart sshd
```

ШАГ 3: УСТАНОВИТЬ FAIL2BAN

ЗАЧЕМ: Автоматически блокировать тех, кто неправильно ввёл пароль 2 раза.

```
# Установить
apt update
apt install -y fail2ban
```

Создать конфиг:

```
nano /etc/fail2ban/jail.local
```

ВСТАВЬ:

```
[DEFAULT]
bantime = 1m
maxretry = 2

[sshd]
enabled = true
```

ЧТО ЭТО ЗНАЧИТ:

- `bantime = 1m` → блокировать на 1 минуту
- `maxretry = 2` → после 2 неудачных попыток

Запустить:

```
systemctl enable fail2ban
systemctl start fail2ban
```

Проверить, что работает:

```
fail2ban-client status sshd
```

ШАГ 4: ЛОГИРОВАНИЕ SSH (AUDITD)

ЗАЧЕМ: Записывать, кто и когда подключался по SSH.

```
# Установить
apt install -y auditd
```

Добавить правила:

```
nano /etc/audit/rules.d/ssh.rules
```

ВСТАВЬ:

```
-w /usr/sbin/sshd -p x -k ssh_exec
-w /etc/ssh/sshd_config -p wa -k ssh_config
```

ЧТО ЭТО ЗНАЧИТ:

- `w /usr/sbin/sshd` → следить за программой SSH
- `p x` → логировать запуск (execute)
- `k ssh_exec` → метка для поиска в логах

Перезапустить:

```
systemctl restart auditd
```

Посмотреть логи:

```
ausearch -k ssh_exec
```