Запрет доступа с УЗ root и служебные УЗ

Прежде чем запретить доступ для root создадим отдельного пользователя `admin` с домашней директорией и с доступом по SSH по ключу (ключ необходимо предварительно сгенерировать см. **эту** статью):

```
useradd -m admin
usermod -aG sudo admin
passwd admin
su admin
mkdir /home/admin/.ssh
cat ssh_key.pub >> /home/admin/.ssh/authorized_keys
chown -R admin:admin /home/admin/.ssh
chmod 700 /home/admin/.ssh
chmod 600 /home/admin/.ssh/authorized_keys
```

Проверяем возможность входа пользователем admin.

Запретим вход по SSH пользователю root, для этого нужно поменять конфиг сервиса sshd:

```
vi /etc/ssh/sshd_config
```

Находим или добавляем (если такой строки нет) следующие строки:

```
PermitRootLogin no
```

Выходим из редактирования с сохранением.

Перезапускаем службу сервиса SSH:

```
systemctl restart sshd.service
```

Далее сбрасываем пароль для УЗ root:

```
sudo passwd -l root
```

Служебные УЗ

УЗ без возможности входа в систему

Такие УЗ могут потребоваться например для проброса портов или SSH туннелирования и т.д. Ниже пример создания такой УЗ:

```
useradd -m portfwd
passwd portfwd
usermod -s /sbin/nologin portfwd
```

Создание УЗ для удаленных бекапов по SCP

На исходной Linux машине, откуда будут забираться бекапы, необходимо создать отдельную специальную УЗ с доступом в определенную папку, в нашем случае это папка `/backup` куда складываются локальные бекапы:

```
adduser --home /backup user_back; chown user_back:user_back /backup; chmod 744 /backup
```

Далее необходимо создать пару ключей для беспарольного входа по этой УЗ:

```
sudo -u user_back ssh-keygen
# Добавить значение из созданного файла *pub в authorized_keys в домашней директории пользователя
user_back
nano /backup/.ssh/authorized_keys
```

Закрытый ключ (без расширения pub) необходимо скопировать на удаленный хост, который будет использоваться для доступа к исходной машине. Далее для копирования можно использовать следующую команду (где 2222 порт SSH):

```
/usr/bin/scp -i /root/.ssh/user_back_key -P 2222 user_back@source.server:/backup/local-backup.tar.gz
/source_server_backup/source-server-backup_$(date +"%d%m%Y").tar.gz
```

Для автоматизации можно добавить эту команду в планировщик задач CRON:

```
crontab -e
```

Для бекапа каждое воскресенье в 00:00 нужно добавить следующую запись в конец файла:

```
0 0 * * 0 /usr/bin/scp -i /root/.ssh/user_back_key -P 2222 user_back@source.server:/backup/local-backup.tar.gz
/source_server_backup/source-server-backup_$(date +"%d%m%Y").tar.gz
```

Для собственного расписания можно использовать этот ресурс https://crontab.guru/

Чтобы удалять архивы старше 30 дней, можно в планировщик также добавить следующую команду:

```
find /source_server_backup/*.gz -type f -mtime +30 -delete
```

Revision #1
Created 12 August 2024 13:41:31 by Boris Rzr
Updated 12 August 2024 13:53:51 by Boris Rzr