

Defesa Born2beRoot

User

Adicionar usuário:

```
sudo adduser <user>
```

Adicionar usuário à um grupo:

```
sudo adduser <user> <group>
```

```
sudo gpasswd -a <user> <group>
```

Remove usuário de um grupo:

```
sudo gpasswd -d <user> <group>
```

Apagar usuário:

```
sudo userdel <user>
```

Verifica o ID do usuário:

```
id <user>
```

Altera a senha do usuário:

```
sudo passwd <user>
```

Verificar os usuários criados:

```
awk -F: '$3 >= 1000 && $3 < 65534 { print $1 }' /etc/passwd
```

Verificar partições

```
lsblk
```

Group

Adicionar grupo:

```
sudo addgroup <group>
```

Apagar grupo:

```
sudo groupdel <group>
```

Verificar ID do grupo:

```
getent group <group>
```

SSH

Verificar status do SSH:

```
sudo service ssh status
```

Reiniciar serviço SSH:

```
sudo service ssh restart
```

Configurar porta SSH:

```
sudo nano /etc/ssh/ssh_config
```

Configurar login com root:

`sudo nano /etc/ssh/sshd_config`

Desativar SSH:

`sudo service ssh stop`

Reiniciar SSH:

`sudo service ssh restart`

Desativar SSH no boot:

`sudo systemctl disable ssh`

Ativar SSH no boot:

`sudo systemctl enable ssh`

UFW

Ativar firewall:

`sudo ufw enable`

Desativar firewall:

`sudo ufw disable`

Verificar status:

`sudo ufw status`

Criar regra (permitir porta):

`sudo ufw allow <porta>`

Deletar regra:

`sudo ufw delete <n>`

Senha

Editar política de senha:

`sudo chage -M 30 -m 2 -W 7 <user>`

Verificar política de senha:

`sudo chage -l <user>`

Validade e expiração de senha:

`sudo nano /etc/login.defs`

Complexidade de senha:

`sudo nano /etc/pam.d/common-password`

Alterar senha:

`sudo passwd <user>`

Hostname

Verificar o hostname (IP):

`hostname`

Alterar o hostname:

`sudo nano /etc/hostname`

Sudo

Verificar se o sudo está instalado

`which sudo`

Regras do sudo:

`sudo nano /etc/sudoers.d/sudo_config`

Servidor

Verificar status do servidor

`sudo systemctl status lighttpd`

Cron

Alterar configurações do CRON

`sudo crontab -u root -e`

Rodar o script ao iniciar

`sudo nano /etc/profile`

Assinatura

`sha1sum <arquivo.vdi>`