setup 2FA with google authenticator for SSH

setting up two factor authentication for ssh with google authenticator is actually very simple. here is how it can be done in just a few steps on ubuntu:

do this as **root** or use `sudo`

```
apt install libpam-google-authenticator
echo "auth required pam_google_authenticator.so" >> /etc/pam.d/sshd
sed -i 's/ChallengeResponseAuthentication no/ChallengeResponseAuthentication
yes/' /etc/ssh/sshd_config
```

now run this for each user to create the google authenticator key for each user:

```
google-authenticator
```

you will be asked a couple of questions, answer them as you please, they are well explained.

the google-authenticator script will show a large QR code.. scan this code with the google authenticator app on your smartphone to set up your key.

now finally restart the sshd service as root

```
systemctl restart sshd
```

from now on you should be asked for your OTP once you have successfully entered your password. Note that this authentication is bypassed when using a private key authentication.

Users that haven't configured google authenticator yet won't be able to login anymore until they have done the google authenticator config.