Step 1 First Install Google authenticator libpam module in kali machine

CMD: sudo apt install libpam-google-authenticator

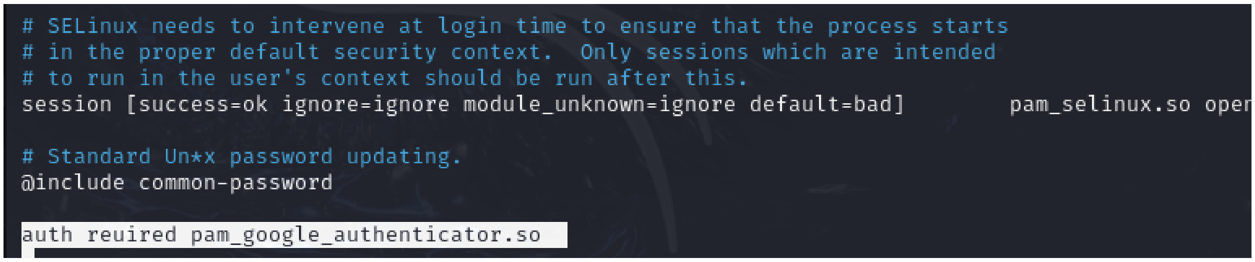
Step 2 Created the setup Emergency Keys using

CMD: google-authenticator

Step 3 Enable the 2FA on SSH

CMD: sudo nano /etc/pam.d/sshd

Add this CMD at the end of the file “auth reuired pam_google_authenticator.so”

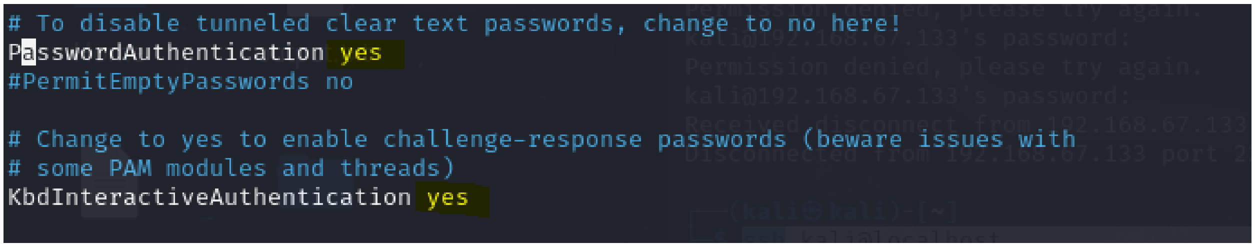


```
# SELinux needs to intervene at login time to ensure that the process starts
# in the proper default security context.  Only sessions which are intended
# to run in the user's context should be run after this.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so open

# Standard Un*x password updating.
@include common-password

auth reuired pam_google_authenticator.so
```

Step 4 Make changes in SSH Configration

CMD: sudo nano /etc/ssh/sshd_config

Change it from no to yes

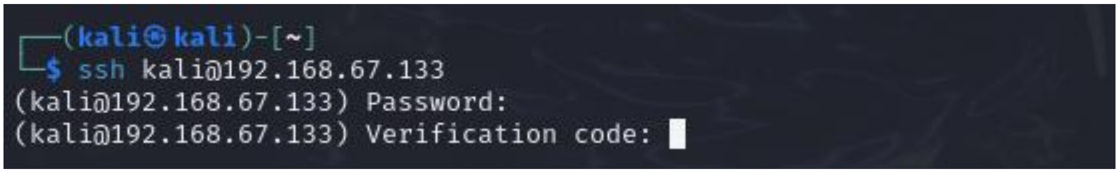


```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication yes
```

Step 5 Restarting SSH Servise

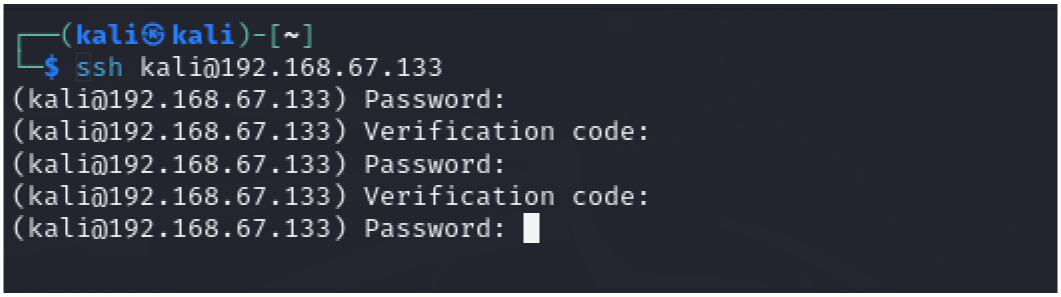
CMD: sudo systemctl restart ssh.service

Step 6 Access the system we need Verification code



```
┌──(kali㉿kali)-[~]
└─$ ssh kali@192.168.67.133
(kali@192.168.67.133) Password:
(kali@192.168.67.133) Verification code:
```

Step 7 We can’t access the System until we have the correct verification code



```
┌──(kali㉿kali)-[~]
└─$ ssh kali@192.168.67.133
(kali@192.168.67.133) Password:
(kali@192.168.67.133) Verification code:
(kali@192.168.67.133) Password:
(kali@192.168.67.133) Verification code:
(kali@192.168.67.133) Password:
```