PREREQUISITO: INSTALLARE liboath0 libpam-oath oathtool

1) $ export HEX_SECRET=$(head -15 /dev/urandom | sha1sum | cut -b 1-30)

2) $ oathtool –verbose –totp $HEX_SECRET –digits=8

Risultato → Hex secret: b5abe8im355c1127sd385a6dd0597x Base32 secret: YWV2RLGFVQUSPLMZTJW5QQQ8 Digits: 8 Window size: 0 Step size (seconds): 30 Start time: 1970-01-01 00:00:00 UTC (0) Current time: 2020-07-26 15:03:57 UTC (1595775837) Counter: 0x32BA74F (53192527)

95354783

3) creare e securizzare “users.oath”:

touch /etc/users.oath chmod 0600 /etc/users.oath

4) aggiungere le seguenti righe (il codice è l'Hex secret) al “users.oath”:

vi /etc/users.oath

Option User Prefix Seed HOTP/T30/6 vage - b5abe8im355c1127sd385a6dd0597x

5) Rimuovere la variabile “HEX_SECRET”:

unset HEX_SECRET

6) Configurare le regole per gli accessi:

vi /etc/security/login_token.conf

Do not require two-factor from here: + : dennis : 1.1.1.0/24

lolnope don't need two-factor at all + : lolnope : ALL

Demand two-factor from everywhere and everyone else - : ALL : ALL

7) editare /etc/pam.d/sshd (per la versione con publickey andare al capitolo successivo “SENZA CHIEDERE LA PASSWORD, USANDO OAUTH + PUBLICKEY ”)

Exceptions from two-factor auth [success=1 default=ignore] pam_access.so accessfile=/etc/security/login_token.conf # Two-factor auth required pam_oath.so usersfile=/etc/users.oath

8) editare /etc/ssh/sshd_config e abilitare “ChallengeResponseAuthentication”

ChallengeResponseAuthentication yes

9) riavviare sshd

Rif: https://wiki.archlinux.org/index.php/Pam_oath
https://dnns.no/two-factor-ssh-using-oathtool-on-ubuntu-18.04.html
https://spod.cx/blog/two-factor-ssh-auth-with-pam_oath-google-authenticator.shtml
https://semjonov.de/post/2016-03/openssh-oath-totp/

SENZA CHIEDERE LA PASSWORD, USANDO OAUTH + PUBLICKEY

7) editare /etc/pam.d/sshd, commentare “@include common-auth” e aggiungere gli altri parametri come di seguito:

@include common-auth

Exceptions from two-factor auth [success=1 default=ignore] pam_access.so accessfile=/etc/security/login_token.conf

Two-factor auth requisite pam_oath.so usersfile=/etc/users.oath

Exceptions from two-factor and publickey auth required pam_sepermit.so

Disallow non-root logins when /etc/nologin exists. account required pam_nologin.so

8) editare /etc/ssh/sshd_config:

UsePAM yes AuthenticationMethods publickey,keyboard-interactive #NOTA! commentando “keyboard-interactive” si disabilita accesso OATH PasswordAuthentication no ChallengeResponseAuthentication yes

9) Riavviare sshd

Rif:
https://www.digitalocean.com/community/tutorials/how-to-set-up-multi-factor-authentication-for-ssh-on-ubuntu-16-04
https://www.insecure.ws/linux/openssh_oath.html#configuring-openssh-with-oath-and-public-keys-2-factor-authentication https://www.insecure.ws/linux/openssh_oath.html
http://delyan.me/securing-ssh-with-totp/
https://serverfault.com/questions/594135/different-requiredauthentications2-for-sshd-and-sftp-subsystem

UTILIZZARE andOTP

a manina si va su “aggiungi dettagli”, nel campo “Etichetta” inserire il nome a vostro piacere della chiave, in “chiave segreta” inserire il “Base32 secret”