How to enable Multi factor authentication for Linux Using Google Authenticator

Step 1: Install the client on a mobile device

Step 2: Install the service on your Linux machine

Debain based:

sudo apt-get –y install libpam-google-authenticator

RHEL Based:

First we need to install the development tools so we have a compiler, and the libraries we need. To do that we’ll use yum to install the “Development Tools” group

sudo yum –y groupinstall “Development Tools”

Now we need to install the pam development package

sudo yum –y install pam-devel

We setup and enable ntp so we can make sure our time is correct. Since we will be using a time based sync.

sudo yum –y install ntp

sudo systemctl start ntpd

sudo systemctl enable ntpd

Now we can download the google authenticator pam module from code.google.com, we will download it to /opt

cd/opt wget https://google-authenticator.googlecode.com/files/libpam-google-authenticator-1.0-source.tar.bz2

unzip, utar, compile the module , and install it:

bunzip2 libpam-google-authenticator-1.0-source.tar.bz2

tar -xvf libpam-google-authenticator-1.0-source.tar

rm -f libpam-google-authenticator-1.0-source.tar

cd libpam-google-authenticator-1.0

make

When the compilation is successfully completed, Google Authenticator can be installed. ( note: this has to be done by a privileged user)

sudo make install

STEP 3: Create the Google authenticator connection for your account.

You can activate the google-authenticator for the root user or any other user. Switch to the user who should use the two-factor authentication and type in:

google-authenticator

{you will get the bar code and your secret key, save them I a secret place for your reference}

you will be prompted to answer a few questions: answer the first two questions with y

do you want authentication to be time-based : y

do you want me to update your “/home/USERNAME/.google\_authenticator” file : y

you can answer the next question according to your needs

you can use the google authenticator app to scan the qr code, or add the account using the secret key and then verification code. Do not forget to print out the emergency scratch codes and store them in a safe place

STEP 4: Create the Google authenticator connection for your account:

To use the module you have to edit the pam, and sshd config files

Vi /etc/pam.d/sshd

Add the following line on top of the file:

auth required pam\_google\_authenticator.so

One more file to edit:

vi /etc/ssh/sshd\_config

Find and change the following line:

ChallengeResponseAuthentication yes

STEP 5: Restart or SSH Service and test the configuration

Now switch back to root and restart SSH server. If you added the two-factor authentication for the root user you can skip the next step.

su root

finally restart the SSH server

/etc/init.d/ssh restart

That’s it! You should now have a SSH server with a two-factor authentication! Test this by openin up a new ssh session to the server, and verify that you can get in before closing out your current ssh session.