Name: Cristian Barreno

Implementing Multi-Factor Authenticator (MFA) on Linux Server - Assignment #7

What is Multi-factor Authentication?

In order to access our laptop, social media accounts, websites, etc. our systems use authentication to know who we claim to be. There are factors that can allow us to authenticate us and log in to our accounts. The factors are the following: something you are, something you know, and something you have. By combining two or more factors of authentication we have a stronger and secure way to access our accounts and continue with our lives.

Today i will go over password authentication with 2 Factor Authentication (2FA)

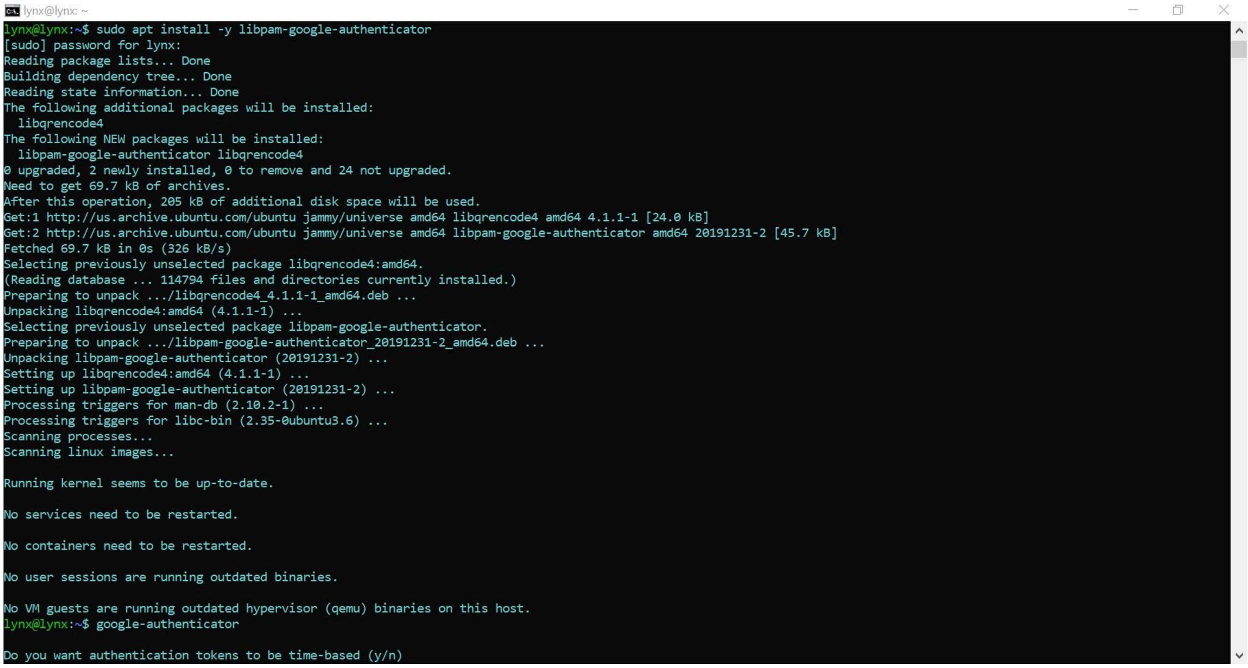
We are going to boot up our Linux VirtualBox Machine, and then we are going to use Secure Shell (SSH) on our computer's Command Prompt.

Step 1. Install Google Authenticator.

Run: `sudo apt install -y libpam-google-authenticator`

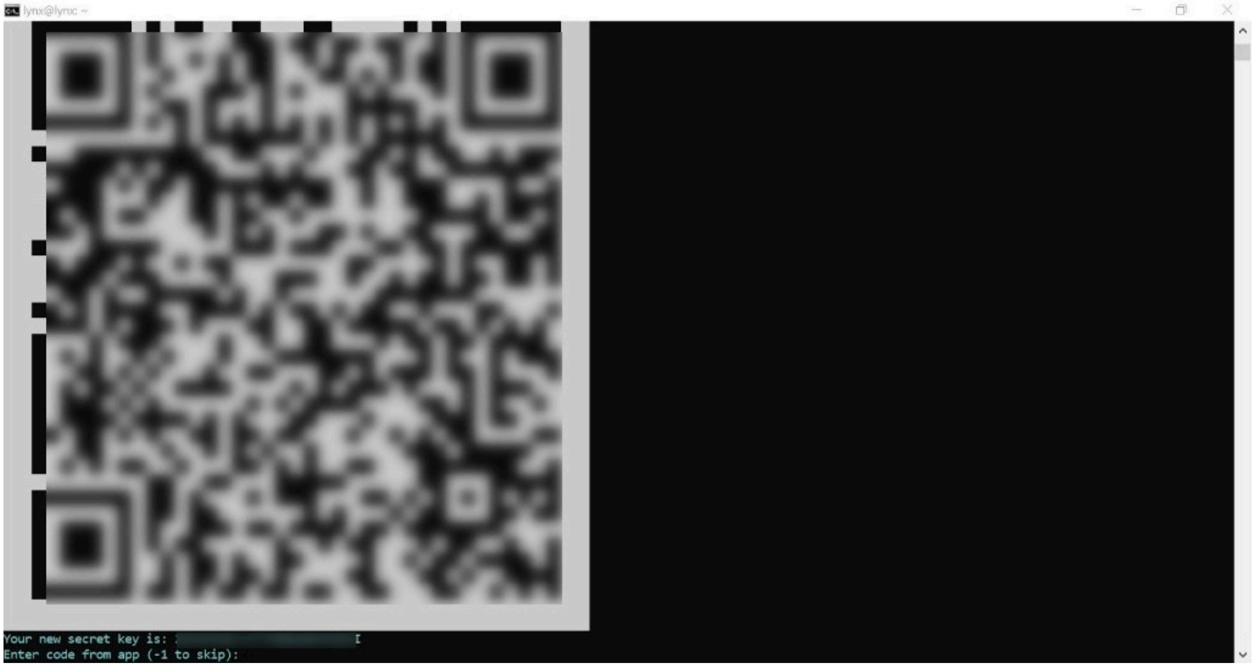
Then run: `google-authenticator`

When asked "Do you want to authenticate tokens to be time-based?" Answer yes.



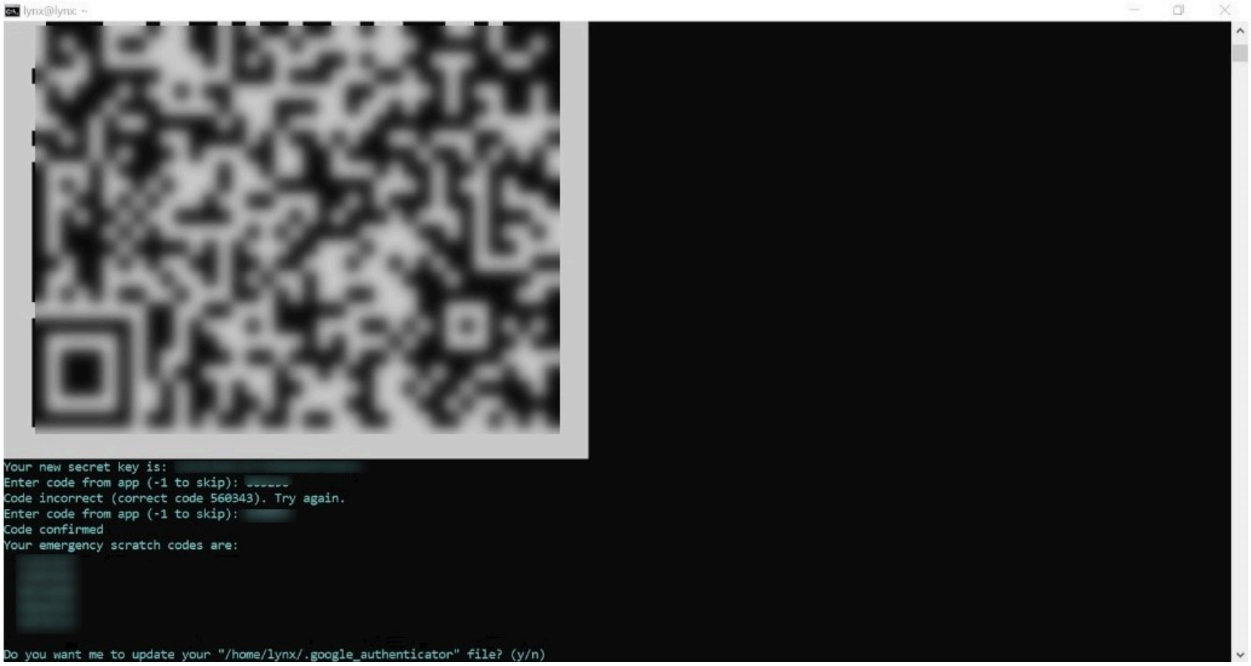
```
lynx@lynx:~$ sudo apt install -y libpam-google-authenticator
[sudo] password for lynx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libqrencode4
The following NEW packages will be installed:
  libpam-google-authenticator libqrencode4
0 upgraded, 2 newly installed, 0 to remove and 24 not upgraded.
Need to get 69.7 kB of archives.
After this operation, 205 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libqrencode4 amd64 4.1.1-1 [24.0 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libpam-google-authenticator amd64 20191231-2 [45.7 kB]
Fetched 69.7 kB in 0s (326 kB/s)
Selecting previously unselected package libqrencode4:amd64.
(Reading database ... 114794 files and directories currently installed.)
Preparing to unpack .../libqrencode4_4.1.1-1_amd64.deb ...
Unpacking libqrencode4:amd64 (4.1.1-1) ...
Selecting previously unselected package libpam-google-authenticator.
Preparing to unpack .../libpam-google-authenticator_20191231-2_amd64.deb ...
Unpacking libpam-google-authenticator (20191231-2) ...
Setting up libqrencode4:amd64 (4.1.1-1) ...
Setting up libpam-google-authenticator (20191231-2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
lynx@lynx:~$ google-authenticator

Do you want authentication tokens to be time-based (y/n)
```

Then you will see a Quick Response (QR) code. From your phone's application store download the Google Authenticator app. Open the app and scan the QR code on your screen.



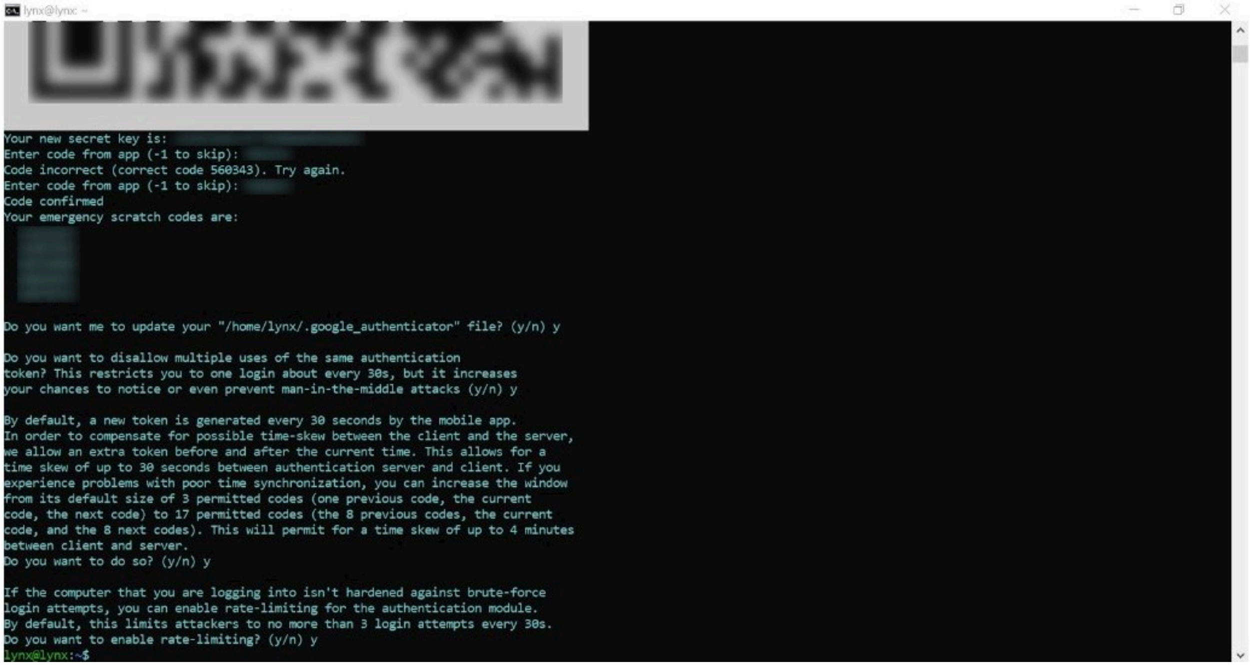
```
Your new secret key is: [redacted]
Enter code from app (-1 to skip):
```

On the Google Authentication app you will see a time sensitive code. Type the code on your computer's screen once prompted to do so.



```
Your new secret key is: [redacted]
Enter code from app (-1 to skip): [redacted]
Code incorrect (correct code 560343). Try again.
Enter code from app (-1 to skip): [redacted]
Code confirmed
Your emergency scratch codes are:
  [redacted]

Do you want me to update your "/home/lynx/.google_authenticator" file? (y/n)
```

Enter Yes to answer the remaining questions.

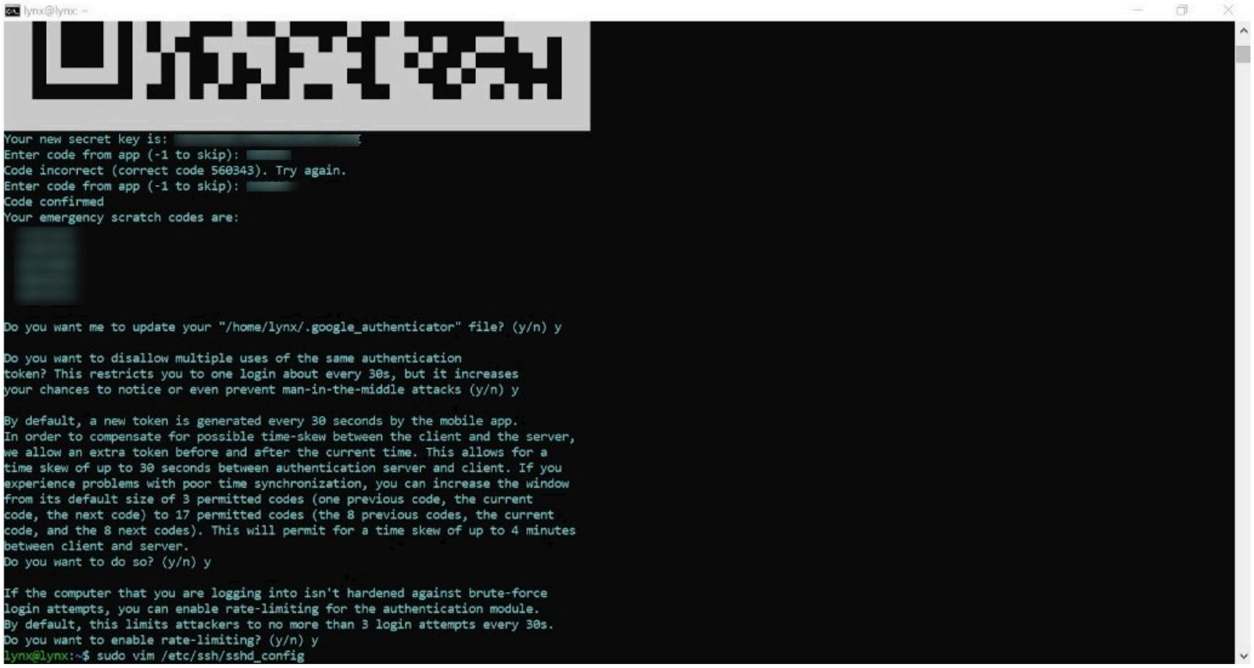


```
Your new secret key is: [redacted]
Enter code from app (-1 to skip): [redacted]
Code incorrect (correct code 560343). Try again.
Enter code from app (-1 to skip): [redacted]
Code confirmed
Your emergency scratch codes are:
  [redacted]


Do you want me to update your "/home/lynx/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
lynx@lynx:~$
```

Step 2: Configure SSH Daemon to use Google Authenticator.

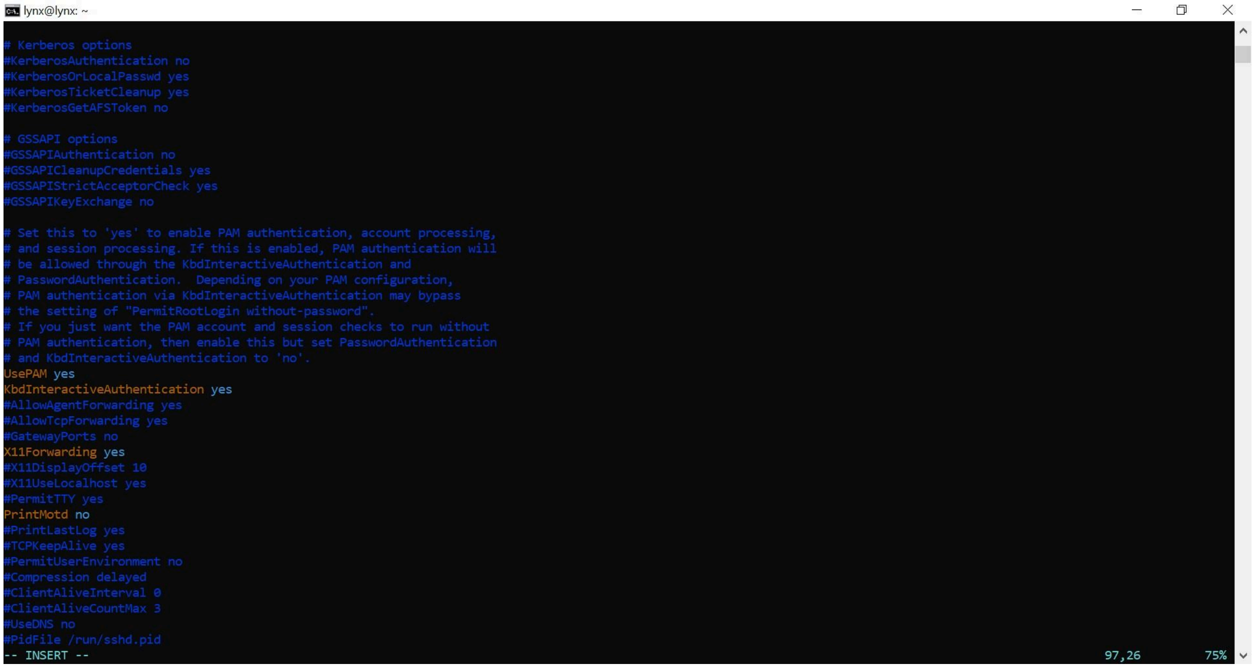
Here we are going to use VIM as our text editor.

Run: `sudo vim /etc/ssh/sshd_config`



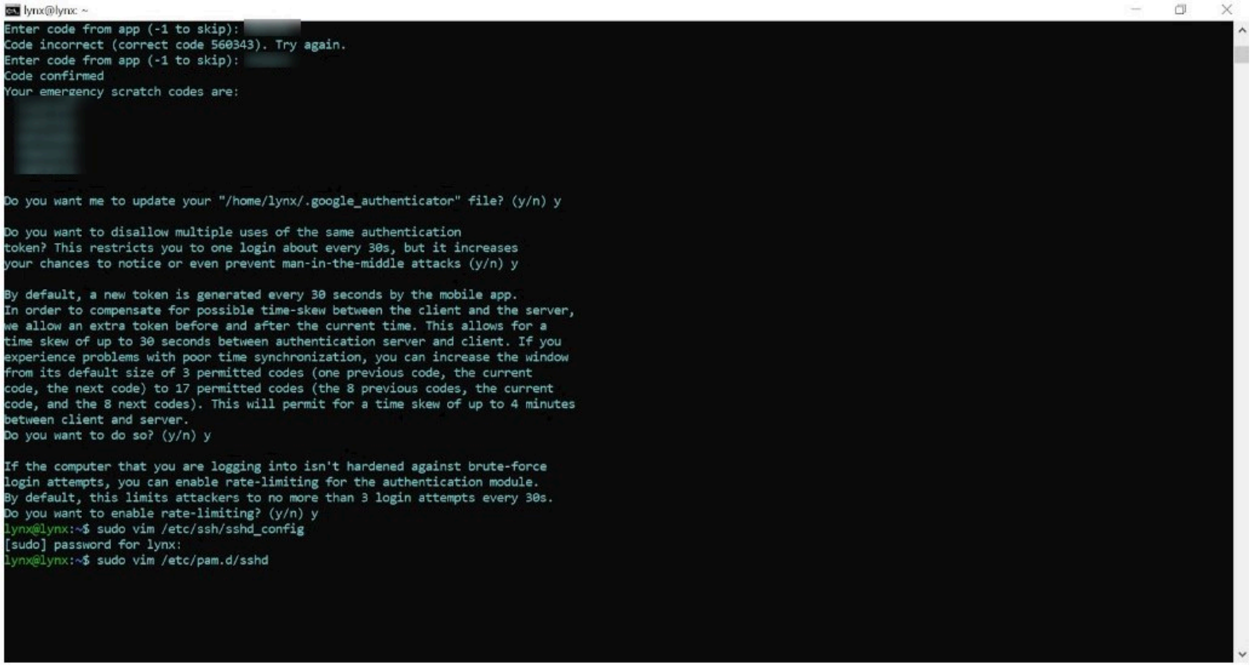
```
Your new secret key is: [redacted]
Enter code from app (-1 to skip): [redacted]
Code incorrect (correct code 560343). Try again.
Enter code from app (-1 to skip): [redacted]
Code confirmed
Your emergency scratch codes are:
  [redacted]


Do you want me to update your "/home/lynx/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
lynx@lynx:~$ sudo vim /etc/ssh/sshd_config
```

Make sure the following parameters and set to yes:
- UsePAM
-kbdInteractiveAuthentication



```
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes
KbdInteractiveAuthentication yes
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
-- INSERT --                                                                                                                                                                97,26          75%
```

Save and close the file
Edit the PAM rule for daemon
Run: `sudo vim /etc/pam.d/sshd`

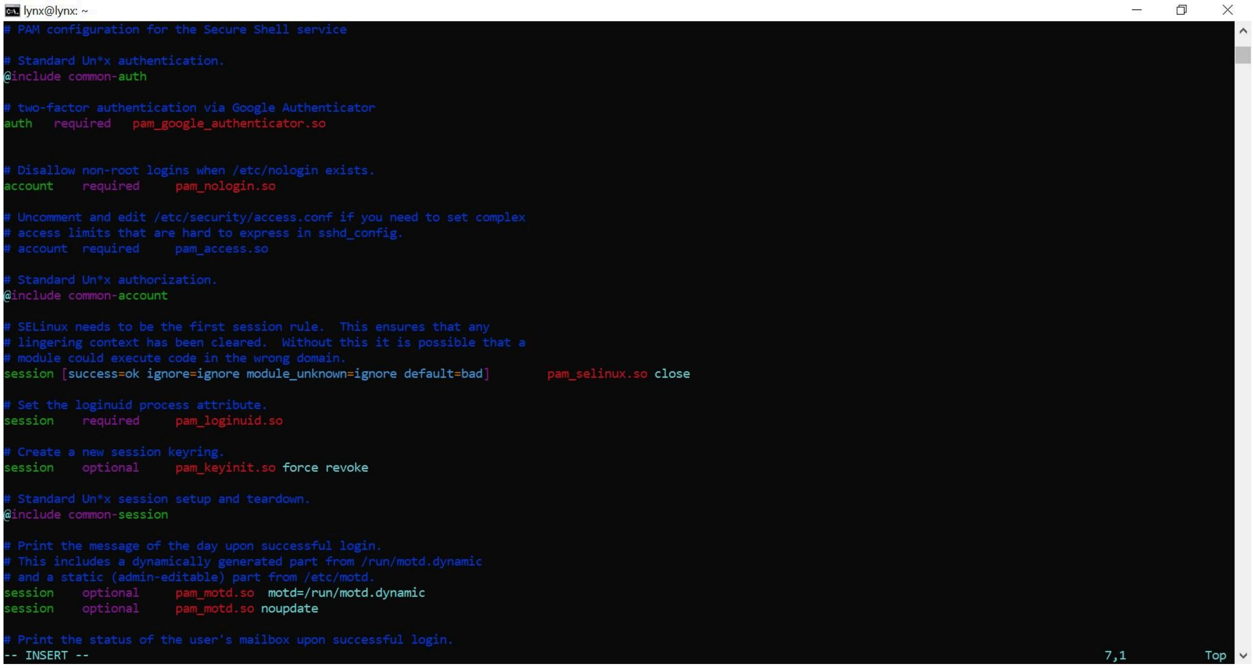


```
Enter code from app (-1 to skip): [redacted]
Code incorrect (correct code 560343). Try again.
Enter code from app (-1 to skip): [redacted]
Code confirmed
Your emergency scratch codes are:
  [redacted]

Do you want me to update your "/home/lynx/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
lynx@lynx:~$ sudo vim /etc/ssh/sshd_config
[sudo] password for lynx:
lynx@lynx:~$ sudo vim /etc/pam.d/sshd
```

To enable 2FA in SSH add the following lines under @include common-auth:

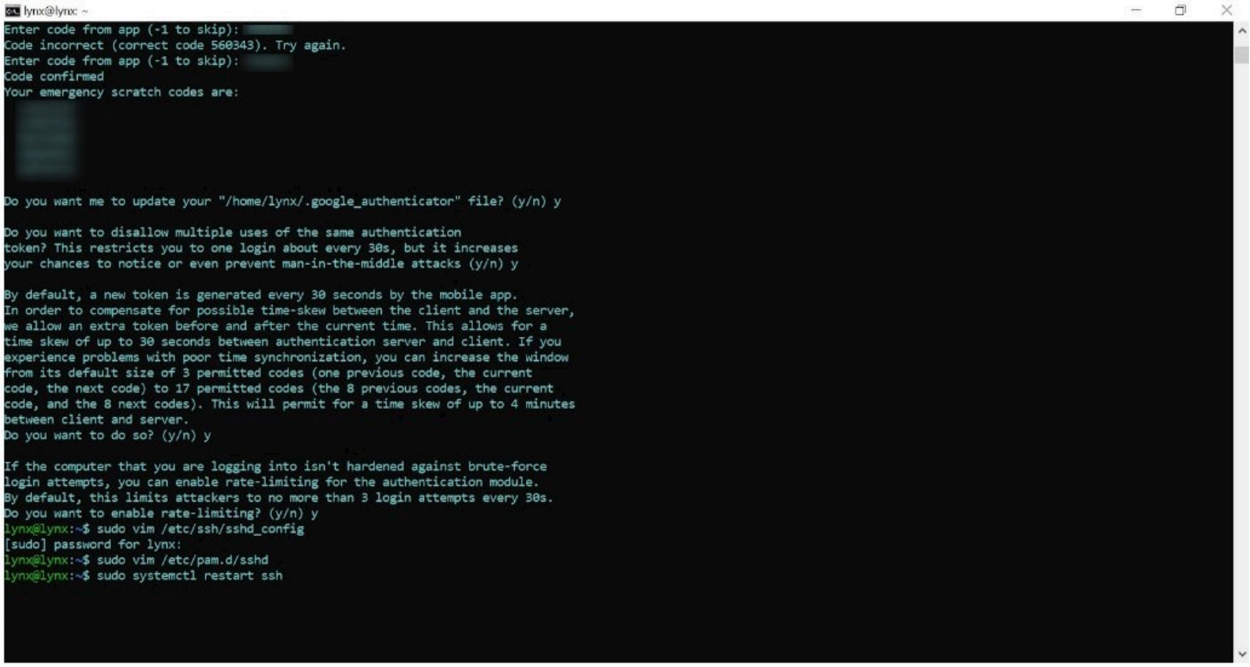
```
# two-factor authentication via Google Authenticator
auth   required   pam_google_authenticator.so
```

Make sure the second line above does not include a # at the beginning once you paste it on VIM.



```
# PAM configuration for the Secure Shell service

# Standard Un*x authentication.
@include common-auth

# two-factor authentication via Google Authenticator
auth   required   pam_google_authenticator.so


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

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account  required     pam_access.so

# Standard Un*x authorization.
@include common-account

# SELinux needs to be the first session rule.  This ensures that any
# lingering context has been cleared.  Without this it is possible that a
# module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so close

# Set the loginuid process attribute.
session    required     pam_loginuid.so

# Create a new session keyring.
session    optional     pam_keyinit.so force revoke

# Standard Un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional     pam_motd.so  motd=/run/motd.dynamic
session    optional     pam_motd.so noupdate

# Print the status of the user's mailbox upon successful login.
-- INSERT --                                                                                                                                              7,1           Top
```

Run: `sudo systemctl restart ssh`

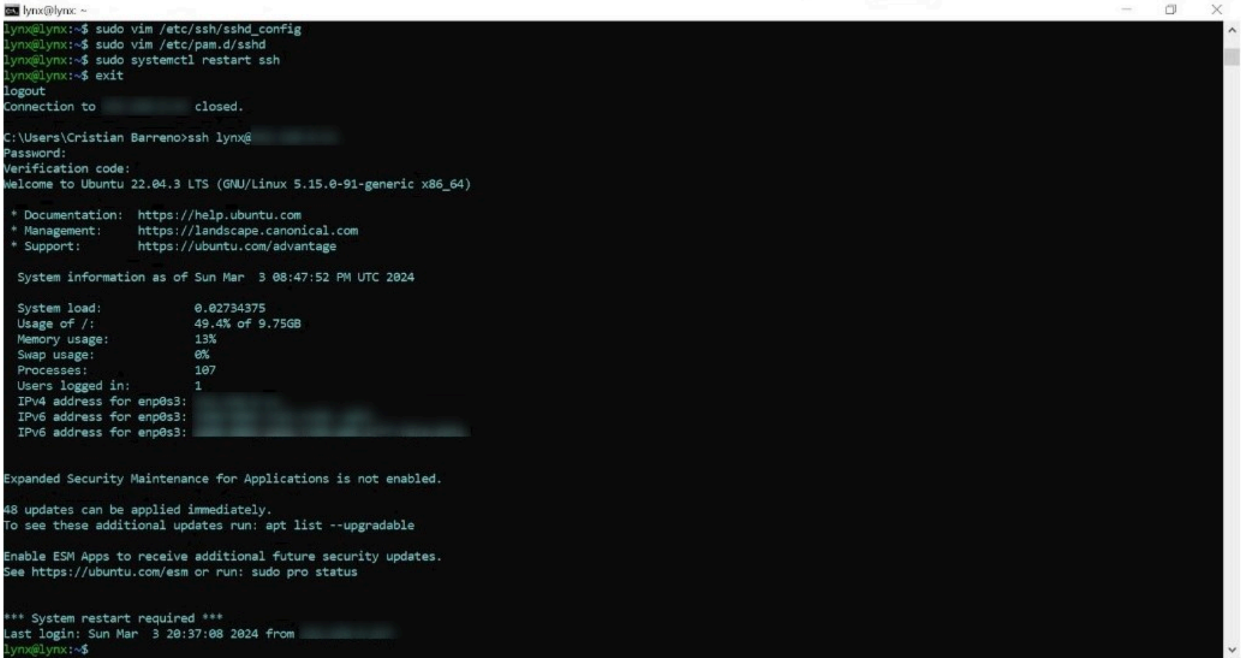


```
Enter code from app (-1 to skip): [redacted]
Code incorrect (correct code 560343). Try again.
Enter code from app (-1 to skip): [redacted]
Code confirmed
Your emergency scratch codes are:
  [redacted]


Do you want me to update your "/home/lynx/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
lynx@lynx:~$ sudo vim /etc/ssh/sshd_config
[sudo] password for lynx:
lynx@lynx:~$ sudo vim /etc/pam.d/sshd
lynx@lynx:~$ sudo systemctl restart ssh
```

Exit the command prompt, and log back in.

After you enter your password to SSH, you will be asked to enter a verification code from your Google Authenticator App.

Congratulations! You used two-factor authentication to log into your linux machine!



```
lynx@lynx:~$ sudo vim /etc/ssh/sshd_config
lynx@lynx:~$ sudo vim /etc/pam.d/sshd
lynx@lynx:~$ sudo systemctl restart ssh
lynx@lynx:~$ exit
logout
Connection to [redacted] closed.

C:\Users\Cristian Barreno>ssh lynx@[redacted]
Password:
Verification code:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Mar  3 08:47:52 PM UTC 2024

  System load:             0.02734375
  Usage of /:              49.4% of 9.75GB
  Memory usage:            13%
  Swap usage:              0%
  Processes:               107
  Users logged in:         1
  IPv4 address for enp0s3: [redacted]
  IPv6 address for enp0s3:
  IPv6 address for enp0s3:


Expanded Security Maintenance for Applications is not enabled.

48 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Sun Mar  3 20:37:08 2024 from [redacted]
lynx@lynx:~$
```