



Raúl Miñana Cots
Andreu Sanz Sanz

SISTEMES DE
GESTIÓ
EMPRESARIAL

2 ° DAM
2023/2024

Tema V

Google Authenticator

Sistemas de Gestión Empresarial | 2023-2024

Andreu Sanz | Raúl Miñana

Tabla de contenidos

Objetivo de la práctica.....	2
¿Qué es la autenticación de dos factores?.....	2
Generar un código QR.....	2
Log.....	2
Activar 2FA en el Server	3
Editar el archivo common authentication.....	3
Log en el Server	3
Editar el archivo de configuración SSH para el PAM.....	3
Editar el archivo de configuración del SSH	3
Reiniciamos el Server	3
Captura de la conexión con SSH desde otro ordenador.....	4

Objetivo de la práctica

El objetivo de esta práctica es aprender cómo añadir una autenticación en dos pasos en nuestro servidor para aumentar la seguridad en el mismo.

¿Qué es la autenticación de dos factores?

La autenticación de dos factores o autenticación de dos pasos, es un proceso de seguridad en dos etapas en el que aseguras tus cuentas con una segunda contraseña, reduciendo así el riesgo de robo de datos. Esto significa que, si deseas iniciar sesión en tu cuenta desde un nuevo dispositivo, necesitarás un segundo código además de la contraseña que hayas elegido para confirmar el acceso.

Generar un código QR



Log

```
Your new secret key is: AKZSVHI465TUDK5C3LIBTH2YBE
Enter code from app (-1 to skip): 156994
Code confirmed
Your emergency scratch codes are:
  27765541
  10552977
  48811510
  88370935
  78736799

Do you want me to update your "/home/andreu/.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
andreu@andreu-ubuntu:~$
```

Activar 2FA en el Server

Editar el archivo common authentication

```
# end of pam-auth-update config
auth required pam_google_authenticator.so nullok
auth required pam_permit.so
```

[Soft wrapping of overlong lines enabled]

Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo

Log en el Server

Tuvimos que cambiar de máquina virtual por problemas técnicos

```
Ubuntu 22.04.3 LTS serverraul tty1

serverraul login: raul
Password:
Verification code: _
```

Editar el archivo de configuración SSH para el PAM

```
# Standard Unix password updating.
@include common-password
auth required pam_google_authenticator.so_
```

Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo

Editar el archivo de configuración del SSH

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

# Kerberos options
#KerberosAuthentication no
```

Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo

Reiniciamos el Server

```
raul@serverraul:~$ sudo systemctl restart sshd.service
raul@serverraul:~$ _
```

Captura de la conexión con SSH desde otro ordenador

```
C:\Users\2DAM_Sanz_Andreu>ssh raul@10.0.219.31
Password:
Verification code:
Verification code:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-87-generic x86_64)

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

System information as of lun 04 dic 2023 17:38:07 UTC

System load:  0.0               Processes:            157
Usage of /:   23.2% of 47.93GB   Users logged in:     1
Memory usage: 6%               IPv4 address for enp0s3: 10.0.219.31
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 50 actualizaciones de forma inmediata.
40 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Last login: Mon Dec  4 17:32:38 2023
raul@serverraul:~$
```