Pràctica 2e: Treballant amb contrasenyes d'accés segures i doble autenticació

1- Objectius de la pràctica

Aquesta activitat té com objectius:

- La creació dúsuaris pels quals es crearan contrasenyes d'accés segures.
- S'incrementarà la seguretat afegint una segona capa d'autenticació (donle autenticació) utilitzant una aplicació de tipus 2FA App.
- Es provarà el funcionament del doble sistema d'autenticació accedint a un servidor SSH correctament configurat i una aplicació instal·lada al mòbil.

Un altre objectiu d'aquesta activitat es treballar els següents resultats d'aprenentatge i continguts marcats al currículum de la UF al DOGC:

- RA1 i C1 →
  - RA1.7 --> Aplica tècniques criptogràfiques en l'emmagatzematge i la transmissió de la informació.
  - C1.6 → Seguretat Lògica

Per desenvolupar aquests objectius i avaluar si s'han adquirit correctament els conneixemens que es demanen:

- L'alumne haurà de llegir i entendre la documentació. Per resoldre qualsevol dubte sobre la documentació, es durà a terme una sessió a classe per explicar els conceptes més importants i resoldre els dubtes que hagin aparegut durant la lectura de la documentació.
- L'alumne haurà de lliurar una pràctica funcionant d'acord a allò que es demani a l'enunciat.

2- Generació de passwords segurs

1. Un password segur hauria de tenir les següents característiques mínimes:
   - Tenir una longitud mínima de 8 caràcters
   - Incloure com a mínim una minúscula
   - Incloure com a mínim una majúscula
   - Incloure com a mínimun número
   - Incloure com a mínim un caràcter especial

2. La distribució Debian del sistema operatiu GNU/Linux permet generar passwords utilitzant l'aplicació **pwgen**. Aquesta ordre permet indicar la quantitat de caràcters, i els tipus de caràcters que volem incloure dins de la contrasenya.

3- Sistema de doble autenticació amb 2FA App (2 Factor Authentication App)

1. Un sistema autenticació doble afegeix una capa de seguretat extra quan es vol accedir al sistema perquè demana autenticar a l'usuari seguint 2 passos:
   - Primer, s'ha d'introduir el nom d'usuari i contrasenya
   - Després s'haura de validar l'usuari introduint un codi que es reberà al mòbil via **SMS** o una aplicació específica per rebre aquest codi que s'hauria d'instal·lar dins del mòbil. Aquest tipus d'aplicacions reben el nom de **2FA App** (2 Facto Authentication App).

2. La doble autenticació via SMS, tot i que utilitzada pels bancs, té algunes vulnerabilitats de manera que serà millor utilitzar una 2FA App com les proporcionades per exemple per **Authy** o per **Google Authenticator**.

3. **Google Authenticator** és el més popular dels sistemes de doble autenticació, és gràtis, força fàcil d'instal·lar i utilitzar per qualsevol usuari, està disponible per ordinadors treballant amb sistemes operatius **Linux/Windows/Apple** i per mòbils o tauletes treballant amb **Android/iOS**. Avui dia molts servidors webs, SSH, etc..., que utilitzen aquest sistema per assegurar la doble autenticació.

4. Per poder fer accesible un servei d'un ordinador via doble autenticació amb Google Autenticator només cal:
   - Instal·lar l'aplicació Google Autenticator dins del mòbil
   - Tenir un lector de codi QR dins del mobil.
   - Instal·lar el programari Google Autenticator dins de l'ordinador que executa el servei al qual es vol accedir via doble autenticació.
   - Configurar el servei l qual es vol accedir via doble autenticació per obligar-lo a afegir doble autenticació via Google Autenticator.

5. Documentació sobre la instal·lació i configuració d'un sistema de doble autenticació amb Google Authenticator pel servei SSH:

   https://ubuntu.com/tutorials/configure-ssh-2fa#1-overview

4- Creació d'un nou usuari amb una contrasenya que utilitzi els criteris bàsics de segurat

a) Afegeix el teu usuari al grup **sudo**. Converteix-te en un usuari **root** i executa:

`gpasswd -a nom_usuari sudo` **(a on nom_usuari** és el nom del teu usuari de sistema)

A continuació surt deixa de ser root i fes un logout per tornar-te a validar en el sistema. Finalment executa:

`id -nG`

i verifica que en la llista de grups dels quals forma part el teu usuari surt el grup **sudo**.

b) Instal·la el programa **pwgen**. Executa:

`sudo aptitude install pwgen`

c) Crea **una** contrasenya de **8** caràcters, que tingui com a mínim una **minúscula**, una **majúscula**, un **número** i un **caràcter especial**. Executa:

`pwgen -y -c -n 8 1`

d) Recorda la contrasenya generada a l'apartat anterior. Crea un usuari del sistema de nom **convidat**. Executa:

`sudo adduser convidat`

Quan et demani la contrasenya escriu la generada a l'apartat anterior. Per la resta de preguntes, prem <Enter> per acceptar l'opció per defecte.

e) Verifica que s'ha creat el nou usuari. Executa:

`cat /etc/passwd | grep convidat`

i comprova que el resultat és similar a aquest:

```
convidat:1001:1001:,,,:/home/convidat:/bin/bash
```

5- Configuració del servei SSH i de Google Authenticator

5.1- Comprova que el servei SSH està instal·lat i funcionant

a) Comprova que el servei SSH està instal·lat. Executa:

```
aptitude search openssh-server
```

i comprova que es mostra el següent resultat:

```
i A openssh-server      - secure shell (SSH) server, for secure access from remote machines
```

b) Comprova que el servei SSH està activat, funcionant i en execució. Executa

```
systemctl status ssh | grep "Active"
```

i comprova que es mostra un resultat similar a aquest (amb data, hora i durada d'acord al moment de l'execució de la instrucció):

```
Active: active (running) since Fri 2022-11-25 12:55:38 CET; 1h 16min ago
```

5.2- Configura el servidor SSH per treballar amb Google Authenticator

a) Instal·la el programari per autenticar usuaris via **Google Authenticator**. Executa:

```
sudo aptitude install libpam-google-authenticator
```

b) Per obligar al servidor SSH a treballar amb **doble autenticació**, modifica el paràmetre **ChallengeResponseAuthentication** del fitxer de configuració del servei SSH **/etc/ssh/sshd_config**. Fes que el seu valor sigui **yes**. Hàuràs de:

- Executar **sudo nano /etc/ssh/sshd_config**
- Buscar el paràmetre **ChallengeResponseAuthentication** que està a la línia **63** de fitxer i canviar **no** per un **yes**.
- Desa i surt del fitxer.

c) Per obligar al servidor SSH a treballar amb **Google Authenticator** afegeix les següents línies al final del fitxer **/etc/pam.d/sshd**:

```
#
# Adding 2FA via Google authenticator
auth required pam_google_authenticator.so
#
```

NOTA: Haurà d'obrir el fitxer amb l'ordre **nano** i treballant amb **sudo**.

d) Reinicia el servei SSH. Executa:

```
sudo systemctl restart ssh
```

5.3- Configura Google Authenticator per accedir al el compte d'usuari convidat amb doble autenticació

a) Accedeix al compte d'usuari convidat del teu servidor. Executa:

```
su - convidat
```

i escriu la contrasenya creada a l'apartat 4 de la pràctica

b) Executa el programa de configuració de **Google Authenticator**:

```
google-authenticator
```

Respon **y** a la pregunta:

```
Do you want authenticaction token to be time based (y/n) y
```

i comprova que es genera un codi QR al terminal del teu equip.

NOTA: Si el codi QR és molt grant, amb **Ctrl -** pots fer-ho més petit.

c) Instal·la dins del teu mòbil l'aplicació **Google Authenticator** des de **Play Store** o **Apple Store**.

d) Executa l'app **Google Authenticator** des del teu mòbil i escaneja el codi QR i apunta el codi que es genera. Compte que el codi té una durada màxima de 30 segons.

e) Entra el codi generat des de l'app de Google Authenticator al mòbil dins de

```
Enter code from app (-1 to skip):
```

Ara els codis que es generin dins del teu mòbil seran vàlids per accedir amb el compte d'usuari **convidat** a qualsevol servei (com per exemple el servei SSH) de la teva màquina que s'hagi configurat per utilitzar doble autenticació.

f) Copia la clau secrat i els codis d'emergència que es generen en un lloc segur. Seran utils si no pots accedir al mòbil per generar codis temporals d'accés.

g) Respon **y** a la resta de preguntes

6- Accés al servidor SSH de la teva màquina des d'un client SSH del company de grup amb el compte d'usuari convidat i doble autenticació.

a) Comprova l'adreça IP de la teva màquina. Executa:

```
ip -4 -br add show dev enp0s3
```

b) Indica al teu company:
- L'adreça IP del teu servidor
- La contrasenya de l'usuari **convidat** que has creat a l'apartat 4 de la pràctica.

c) Demana al teu company que faci un **ping** a la màquina per comprovar que hi ha connectivitat.

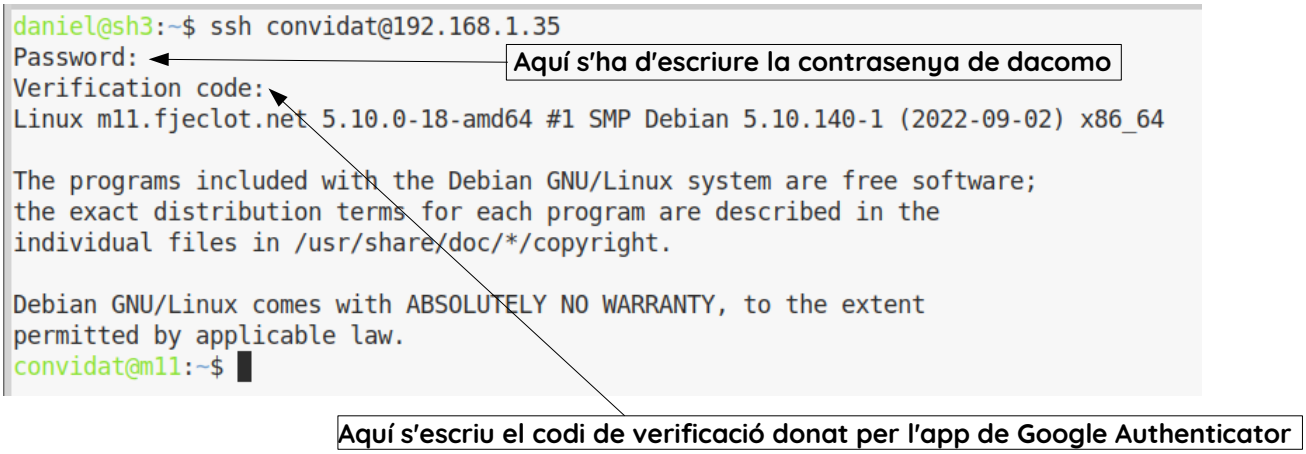
d) Envia per **Whatsapp** o **Telegram** al teu company el codi actual de **Google Authenticator** per l'usuari convidat dins de la teva màquina. Compte que només té un durada de 30 segons.

e) Demana al teu company que accedeix a la teva màquina via SSH utilitzant el compte d'usuari **convidat**. El teu company haurà d'executar des de la seva màquina:

ssh convidat@adreça_ip

a on **adreça_ip** és l'adreça IP de la teva màquina que has trobat a l'apart **a)**. A continuació haurà d'indicar la contrasenya i després el codi de verificació.

Aquí poso una captura d'un exemple d'accés:



Forma de lliurament de la pràctica

1- Activitat en grups de 2 persones

2- Comprovació:

- Un membre del grup haurà de fer una connexió al servidor SSH de l'altre membre del grup utilitzant el compte de **convidat**. L'accés haurà de complir que:
  - La contrasenya de convidat ha de ser segura
  - L'accés es fa utilitzant doble autenticació
- S'haurà de repetir el procés però invertint els roles de qui fa de servidor i qui fa de client.

3- Dates de lliurament:

- Setmana del 9-1-23 al 13-1-23 100% de la nota
- Despŕe del dia 13-1-23: 50% de la nota