SMR – Seguridad Informática

UT N.º 1 – Introducción a la seguridad informática

Actividad	
1	Autentificación en 2 pasos en GNU/Linux, con *token*
REQUISITOS	
• Máquina virtual Debian sin entorno gráfico • Un *pendrive,* para usar como *token* de acceso	

Planteamiento

Vamos a configurar nuestra máquina virtual para que sólo nos permita entrar en nuestra cuenta si cumplimos estas dos condiciones:

1. Introducir nuestro usuario y contraseña (como se hace habitualmente)
2. Tenemos conectado a la máquina un pendrive dado.

Deben cumplirse **ambas** condiciones: si no está el pendrive conectado, no nos debe dejar acceder a nuestra cuenta. Si no introducimos bien nuestro usuario y contraseña, tampoco.

De esta manera, combinamos *algo-que-sabes* con *algo-que-tienes* para aumentar la seguridad en el acceso a la máquina.

NOTA: este tutorial está desarrollado pensando que ya tienes el pendrive en tu poder. Si no es así, puedes seguir los pasos de instalación del software y, más adelante, usar el comando `pamusb-conf` para configurar el pendrive para tu usuario.

Nota: este tutorial está desarrollado pensando que ya tienes el pendrive en tu poder. Si no es así, puedes seguir los pasos de instalación del software y, más adelante, usar el comando `pamusb-conf` para configurar el pendrive para tu usuario.

Desarrollo

Sigue los siguientes pasos para desarrollar esta práctica:

1. Abre el programa de virtualización (VirtualBox). Crea una máquina virtual según el tutorial facilitado por el profesor, usando la distribución que te indique el mismo.
2. En la sección USB de VirtualBox correspondiente a tu máquina virtual activa el servicio USB 3.0.
3. Inserta en el ordenador el *pendrive* que vas a usar como *token* para la autentificación.
4. En la misma sección de USB de VirtualBox, añade un filtro para que la máquina virtual tenga acceso al pendrive (si no puedes añadir el filtro, probablemente tu cuenta en el ordenador necesita ser añadida al grupo especial *vboxusers* con el comando

`sudo usermod -aG vboxusers NOMBRE_USUARIO`, **pero tú no podrás hacerlo. Pide al profesor que lo haga por ti**).

5. Inicia la máquina virtual y entra en tu cuenta con tu nombre de usuario y contraseña.

6. Comprueba que tu máquina virtual tiene acceso al pendrive: ejecuta el comando `ls /dev` para ver los dispositivos disponibles. Tendrás tu unidad de disco básica, ***sda***, con sus particiones *(**sda1***, ***sda2***, etétera). Tu pendrive estará identificado como la última de las unidades sd* (probablemente ***sdb***) y seguramente podrás ver también las particiones que contenga, como ***sdb1***, etc.

7. Para poder hacer esta práctica, necesitamos instalar en la máquina un paquete de software especial: **libpam-usb**. Durante varios años el paquete dejó de ser mantenido por su creador, y acabó desapareciendo de los repositorios estándar de Debian. Pero un técnico lo ha retomado para volver a hacerlo activo y, aunque no está aún en los repositorios oficiales de Debian, al menos ya se puede instalar usando su repositorio personal. El primer paso es configurar tu sistema para aceptar la clave de cifrado de su repositorio:
   ```
   sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 913558C8A5E552A7
   ```

8. A continuación añadimos su repositorio personal a nuestro archivo `/etc/apt/sources.list`. Edita dicho archivo con el comando `sudo nano /etc/apt/sources.list` y añade al final la siguiente línea:
   ```
   deb https://apt.mcdope.org/ ./
   ```

9. Guarda el archivo y cierra el editor.

10. Ahora puedes actualizar la caché de paquetes e instalar el paquete como lo haríamos normalmente:
    ```
    sudo apt update
    sudo apt install libpam-usb
    ```

11. Añade tu pendrive como dispositivo para autentificar:
    ```
    sudo pamusb-conf --add-device llave-de-julio
    ```

    Si tienes más de un dispositivo disponible, se te mostrarán, para que selecciones el que quieras usar. El último argumento es un nombre que usaremos para referirnos al pendrive. Yo he puesto «llave-de-julio», pero puedes poner lo que quieras.

12. Añade todos los usuarios que requerirán usar un pendrive para entrar al sistema (en este caso, al menos tu propio nombre de usuario):
    ```
    sudo pamusb-conf --add-user julio
    ```

    El programa te preguntará qué token quieres usar (en esta práctica sólo debería aparecer uno, porque sólo hemos definido uno en el paso 7).

13. Si todo está bien, en este momento el sistema te autentificará con contraseña O con el pendrive. Es decir, si el pendrive está conectado, ni siquiera te pedirá la contraseña. Vamos a cambiarlo para que nos pida AMBAS cosas. Edita el archivo */etc/pam.d/common-auth*. Este archivo contendrá una línea como esta:
    ```
    auth    sufficient      pam_usb.so
    ```

Debes cambiarla a:

```
auth    required        pam_usb.so
```

14. Ahora, tanto para conectarte a tu cuenta como para ejecutar cualquier comando con *sudo*, deberás tener el pendrive conectado e introducir tu contraseña. ¡Compruébalo!
    Ten en cuenta que si has hecho `sudo su` correctamente, puedes sacar el pendrive y volver a hacerlo sin problemas, porque *sudo* recuerda durante un tiempo que te has autentificado correctamente, y no hace ninguna comprobación.

Ampliaciones optativas

- Una vez que has configurado todo correctamente, no podrás conectarte a la máquina por ssh fácilmente, ya que la autentificación remota no funcionará por no disponer del *pendrive*. Investiga cómo resolver esto.
- Investiga cómo hacer que el sistema realice alguna acción (por ejemplo, cerrar tu sesión) al retirar el pendrive de la máquina.

Preguntas

1. ¿Cómo podrías hacer algo similar para una máquina Windows?
2. ¿Puedes jugar con el PAM y hacer combinaciones más complejas? ¿Por ejemplo, que pida el *pendrive* para hacer *sudo* pero no para hacer *login*?