Lab 1.1: Configurar el sistema con sudo

Es muy peligroso ejecutar una **terminal de root** a menos de que sea absolutamente necesario: un solo error de tipeo o de otro tipo puede causar daños graves (incluso no recuperables).

Por lo tanto, el procedimiento recomendado es configurar el sistema de tal forma que comandos únicos puedan ser ejecutados con privilegios de superusuario, a través del mecanismo de **sudo**. Con **sudo** el usuario necesita conocer su propia clave solamente y nunca la del usuario root.

Si usted está usando una distribución como **Ubuntu**, es posible que no necesite realizar este laboratorio para tener **sudo** configurado de forma apropiada para el curso. Sin embargo, todavía necesita asegurarse de comprender el procedimiento.

Para comprobar si su sistema ya está configurado para permitir que la cuenta de usuario que está usando ejecute **sudo**, ejecute un comando simple como el siguiente:

```
$ sudo ls
```

Se le debería pedir la clave de usuario y luego el You should be prompted for your user password and then el comando sería ejecutado. Si en cambio obtiene un mensaje de error, entonces necesitará realizar el siguiente procedimiento.

Inicie una terminal de root a través del comando **su** y luego provea la clave de **root**, no su clave de usuario.

En todas las distribuciones recientes de **Linux** usted debería ir al subdirectorio /etc/sudoers.d y crear un archivo, generalmente con el nombre del usuario al cual root desea concederle acceso a **sudo**. Sin embargo, esta convención no es realmente necesaria, ya que **sudo** escaneará todos los archivos en este directorio. El archivo puede contener algo tan simple como lo siguiente:

```
estudiante ALL=(ALL)  ALL
```

si el usuario es `estudiante`.

Una práctica antigua (la que aún funciona) es agregar la línea al final del archivo /etc/sudoers. Lo más recomendable es hacerlo con el programa **visudo**, ya que se ocupa de que usted esté usando la sintaxis adecuada mientras edita.

Es posible que necesite configurar los permisos adecuados en el archivo, de la siguiente forma:

```
$ chmod 440 /etc/sudoers.d/estudiante
```

Tenga en cuenta que algunas distribuciones **Linux** pueden requerir permisos `400` en vez de `440` .

Luego de haber realizado esos pasos, salga de la consola root con `exit` e intente de nuevo `sudo ls` .

Hay muchas otras cosas que un administrador puede configurar en **sudo**, incluyendo permisos para usuarios específicos, limitar las búsquedas a ciertos directorios, etc. El archivo /etc/sudoers está muy bien autodocumentado.

Sin embargo, hay un ajuste adicional que recomendamos altamente que realice, aún si su sistema ya tiene configurado **sudo**. La mayoría de las distribuciones establecen directorios diferentes para los directorios en donde se encuentran los ejecutables de los usuarios normales y los de root. En particular los directorios /sbin y /usr/sbin no son encontrados en las búsquedas, ya que **sudo** hereda el `PATH` del usuario, no del superusuario.

Por lo tanto, en este curso estaremos constantemente recordándole la ruta completa de varias herramientas de administración; cualquier otra mejora en cuanto a la seguridad de esta implementación probablemente no valdrá la pena (como intentar esconder los binarios del superusuario, por ejemplo).

En consecuencia, sugerimos agregar la siguiente línea al archivo .bashrc en su directorio de usuario:


```
PATH=$PATH:/usr/sbin:/sbin
```

No es necesario que reinicie, en vez de eso, puede salir de la sesión y entrar nuevamente, lo cual será completamente efectivo.

