SEGURIDAD: SUDO

Configuración comando "sudo"

- La configuración de “sudo” está en el fichero:
  /etc/sudorers
- Si la sintaxis es incorrecta y salvamos SIN VALIDAR

el comando “sudo” no se podrá ejecutar NUNCA MÁS
y quedaría invalidado el acceso a “root” via sudo
(solo se podría acceder a root vía “su” o vía “login”)

- Por ello: el archivo /etc/sudorers se medifica mediante la mediación de un programa especial llamado “visudo”

que analiza la sintaxis de /etc/sudorers antes de salvarlo

```
# sudo -i
# visudo
```

NUNCA USAR: # vi /etc/sudorers

Configuración comando "sudo"

- "visudo" llama al editor por defecto del sistema , por ejemplo "nano", aunque podemos cambiar a "vi":

```
# update-alternatives   -config editor
```

<user><host>= (<runas_user>) <command>

Ejemplo de regla:

pyromikel ALL = (ALL) ALL

El usuario pyromikel, en cualquier host (ALL), puede ejecutar, de aquellos comandos propiedad de cualquier usuario (ALL), cualquiera de dichos comandos (ALL)

Configuración comando "sudo"

Otro ejemplo...

- **Crear 2 usuarios de prueba : zipi y zape**

 # adduser zipi ...
 # adduser zape ...
 # cat > /home/zipi ...
echo "Hola Mundo"

- **Hacemos un "holaMundo" propiedad de zipi**

 # chown zipi:zipi holaMundo

- **Permitimos la ejecución del "holaMundo" solo a zipi**

 # chmod 700 holaMundo

Configuración comando "sudo"

Ahora comprobamos que zape no puede ejecutar el "holaMundo" de zipi:

 # zape@servidor > /home/zipi/holaMundo

-bash: /home/zipi/holaMundo: Permission denied

Añadimos nueva regla a /etc/sudoers para que zape pueda EXCLUSIVAMENTE ejecutar el holaMundo de zipi:

zape ALL = (zipi) /home/zipi/holaMundo

Configuración comando "sudo"

Ahora tratamos de ejecutar el holaMundo usando el comando sudo (sin opciones):

 # zape@servidor > sudo /home/zipi/holaMundo
Sorry, user zape is not allowed to execute '/home/zipi/holaMundo' as root on servidor.

Ahora tratamos de ejecutar el holaMundo con el usuario zape haciendo sudo como el usario zipi:

 # zape@servidor > sudo –u zipi /home/zipi/holaMundo
Hola Mundo

Configuración comando "sudo"

En la shell podemos ejecutar una sentencia “for”:

```
# for indice in {1..10}
   do
        echo “Iteración número $indice”
   done
```

Vamos a hacer 10 copias de holaMundo desde la shell usando un comando for:

```
# cd /home/zipi
# for  indice in  {1..10}
   do
        cp holaMundo holaMundo_$indice
  done
```

Configuración comando "sudo"

Ahora vamos a crear una regla en /etc/sudoers para que zape tenga pueda hacer sudo y ejecutar cualquiera de los nuevos comando de la forma holaMundo_X :

Creamos un alias para los comandos:

```
Cmnd_Alias HOLAMUNDOS = \
                /home/zipi/holaMundo_*
```

Ahora modificamos la regla anterior teniendo en cuenta el nuevo alias:

```
zape ALL = (zipi) HOLAMUNDOS
```

Configuración comando "sudo"

Ahora, el usuario zape puede ejecutar todas las copias de holaMundo haciendo sudo (como usuario zipi):

```
zape@BRAINIAC > cd /home/zipi
zape@BRAINIAC > for indice in {1..10}; do
                                    sudo –u zipi holaMundo_*
                                done
```

Vamos a modificar el sudo para que, en general nunca pida clave (INSEGURO!!!)

```
Defaults  !authenticate
```

Configuración comando "sudo"

Si quiero que NO me pida clave para:
holaMundo_3 hasta holaMundo_7
... pero me pida clave SIEMPRE para el resto...

1) **Elimino Defaults !authenticate**
2) **Añado Defaults timestamp_timeout=0**
3) **Añado un nuevo alias:**

```
Cmnd_Alias  HOLAMUNDOS_3TO7 \
        /home/zipi/holaMundo_[3-7]
```

4) **Modifico la regla de acceso:**

```
zape ALL = (zipi) PASSWD:HOLAMUNDO,   \
                        NOPASSWD: HOLAMUNDO_3TO7
```

Configuración comando "sudo"

```
zape@servidor> cd /home/zipi
zape@servidor > for indice in {1..10}
                        do
                                sudo –u zipi holaMundo_*
                        done
```

???