

Guía de Laboratorio: Uso de Scripts de Consola

Módulo I: Introducción y Fundamentos de Ciberseguridad.

Nombre del estudiante: Julian Rivera-Pineda

Objetivo: Comprender los conceptos básicos en el uso de scripts de consola que permitan automatizar tareas.

Creación de Script para Inhabilitación de Usuarios en Linux

Prerrequisitos

- Se recomienda utilizar Kali Linux para esta práctica.
- Su sistema operativo debe contar con un usuario *testuser*. Puede proceder a crearlo ejecutando el siguiente comando con permisos de superusuario.

```
(kali㉿kali)-[~/Documents]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~/Documents]
# useradd testuser
```

Indicaciones

1. Con el editor de texto nano, cree un nuevo documento de texto.

```
(kali㉿kali)-[~/Documents]
# nano deshabilitar_usuario_testuser.sh
```

2. Agregar la siguiente instrucción al inicio del documento

```
GNU nano 7.2 deshabilitar_usuario_testuser.sh
#!/bin/zsh
```

esta instrucción permite indicar la ruta absoluta del interprete a utilizar.

3. Agregar las siguientes instrucciones

```
usermod -L testuser
chage -E0 testuser
usermod -s /sbin/nologin testuser
```

Su archivo debe lucir como se muestra en la imagen

```
GNU nano 7.2 deshabilitar_usuario_testuser.sh
#!/bin/zsh

usermod -L testuser
chage -E0 testuser
usermod -s /sbin/nologin testuser
```

4. Proceda a guardar el archivo con la secuencia de comandos CTRL + O, ENTER (para guardar) y CTRL + X (para salir).

```
File Name to Write: deshabilitar_usuario_testuser.sh
^G Help          M-D DOS Format   M-A Append
^C Cancel        M-M Mac Format   M-P Prepend
```

5. Otorgue permisos de ejecución al script

```
(root@kali)-[/home/kali/Documents]
# chmod +x deshabilitar_usuario_testuser.sh
```

6. Ejecute el script

```
(root@kali)-[/home/kali/Documents]
# ./deshabilitar_usuario_testuser.sh
```

7. Valide que el usuario se encuentra deshabilitado.

```
(root@kali)-[/home/kali/Documents]
# passwd --status testuser
testuser L 2023-07-18 0 99999 7 -1
```

```
(root@kali)-[/home/kali/Documents]
# chage -l testuser
Last password change           : Jul 18, 2023
Password expires                : never
Password inactive               : never
Account expires                 : Jan 01, 1970
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

```
(root@kali)-[/home/kali/Documents]
# cat /etc/passwd | grep testuser
testuser:x:1001:1001::/home/testuser:/sbin/nologin
```

8. Adjunte en esta guía, una captura de pantalla de donde se evidencie la salida de las tres instrucciones del paso anterior junto con la hora en que finalizó la práctica.

```
root@kali: ~kali
File Actions Edit View Help

(root@kali)~[~kali]
# passwd --status testuser
testuser L 2023-07-19 0 99999 7 -1

(root@kali)~[~kali]
# chage -l testuser
Last password change           : Jul 19, 2023
Password expires                : never
Password inactive              : never
Account expires                : Jan 01, 1970
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

(root@kali)~[~kali]
# cat /etc/passwd | grep testuser
testuser:x:1001:1001::/home/testuser:/sbin/nologin

(root@kali)~[~kali]
# date
Wed Jul 19 12:22:53 AM EDT 2023

(root@kali)~[~kali]
#
```

Nota: Reemplace esta imagen por la suya.

9. Conteste las siguientes interrogantes:

- ¿Cuál es el propósito del comando `usermod -L <username>`?

Lock the user account (Bloquea la Cuenta de usuario)

- ¿Qué acción realiza el comando `chage -E0 <username>`?

Set the date or number of days since January 1, 1970 on which the user's account will no longer be accessible. (Establece la fecha o el número de días desde el 1 de enero de 1970 en que la cuenta del usuario dejará de ser accesible. En este caso 0 días)

- ¿Cuál es el propósito de especificar `/sbin/nologin` como consola de inicio de sesión con el comando `usermod -s`?

When `/sbin/nologin` is set as the shell, if user with that shell logs in, they'll get a polite message saying 'This account is currently not available.' This message can be changed with the file `/etc/nologin.txt`. (Cuando se establece `/sbin/nologin` como shell, si un usuario con ese shell inicia sesión, recibirá un mensaje de cortesía diciendo 'Esta cuenta no está disponible actualmente'. Este mensaje puede cambiarse con el archivo `/etc/nologin.txt`.)

- ¿Qué significa la L que aparece en la salida del comando `passwd --status <username>`?

The second field indicates if the user account has a locked password (L) (El segundo campo indica si la cuenta de usuario tiene una contraseña bloqueada (L))

- ¿Qué modificaciones haría al script para que tome el nombre de usuario como parámetros de entrada?

Las modificaciones son las siguientes:

```
GNU nano 7.2 deshabilitar_usuario.sh
#!/bin/zsh
#### Modificaciones para que tome un usuario como parametro
#### $1 es el nombre del usuario

if [ -n "$1" ]
then
    usermod -L $1
    chage -E0 $1
    usermod -s /sbin/nologin $1
    if [ $? -eq 0 ]; then
        echo "Imprimiendo el estatus del password del usuario:"
        echo "Estatus: $(passwd --status $1) "
        echo "Imprimiendo el estatus de expiracion del password"
        echo "Expiracion: $(chage -l $1)"
        echo "Imprimiendo la informacion del usuario desde /etc/passwd"
        echo "Info Usuario $(cat /etc/passwd | grep $1)"
    else
        echo "Se produjo un error en la ejecucion de los comandos "
    fi
else
    echo "Forma de uso: $0 nombre_de_usuario"
fi
```

Ejemplo de ejecución del nuevo script **deshabilitar_usuario.sh** sin parámetros:

```
(root@kali) [kali]
# ./deshabilitar_usuario.sh
Forma de uso: ./deshabilitar_usuario.sh nombre_de_usuario
```

Ejemplo de ejecución del nuevo script **deshabilitar_usuario.sh** con parámetros:

```
(root@kali)-[~kali]
# useradd jessita

(root@kali)-[~kali]
# ./deshabilitar_usuario.sh jessita
Imprimiendo el estatus del password del usuario:
Estatus: jessita L 2023-07-19 0 99999 7 -1
Imprimiendo el estatus de expiracion del password
Expiracion: Last password change : Jul 19, 2023
Password expires : never
Password inactive : never
Account expires : Jan 01, 1970
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
Imprimiendo la informacion del usuario desde /etc/passwd
Info Usuario jessita:x:1002:1002::/home/jessita:/sbin/nologin

(root@kali)-[~kali]
#
```

Nota 1: Código fuente de esta practica disponible en <https://github.com/xtecuan/guia2-DCS2023.git>

10. Guarde este documento como PDF y súbalo al aula virtual.