

Evaluación práctica – Cripto y SecInfo

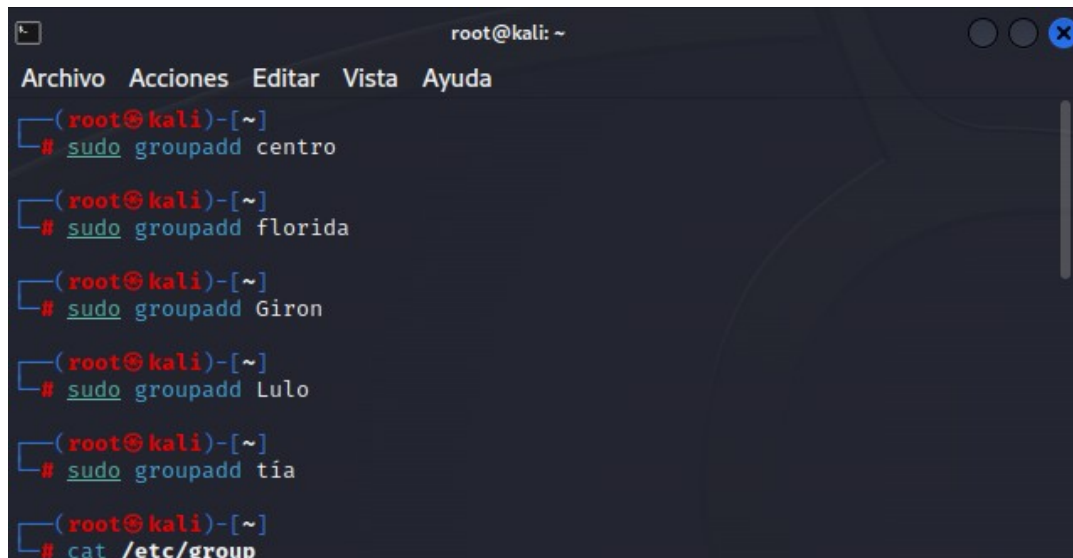
NRC 10391

ID: 00042744

Nombre: Santiago Andres Del Valle Pinilla

El laboratorio se hará en Kali Linux debido a problemas de compatibilidad con Ubuntu Server ,
agradecemos vuestra comprensión.

1. Usted es el oficial de ciberseguridad de la organización RESTAURANTES MI GORDITO S.A. Una red compuesta por 5 restaurantes en diferentes lugares de la ciudad. Esta empresa cuenta con usuarios que quieren que usted le organice y con información que necesita que cada uno de estos usuarios acceda de acuerdo con los respectivos permisos que el dueño haya definido.
2. Su enlace es el sobrino de la dueña, el señor Lulo Gordon, la dueña es muy ocupada y no dispone de tiempo para dar las instrucciones necesarias, el joven Lulo estaba sin laburo y le cayó como anillo al dedo el encargo que le hizo su tía.
3. El sistema operativo con el que se cuenta es Ubuntu Server 22.04, sin interfaz gráfica por supuesto.

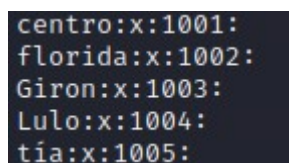


```

root@kali: ~
Archivo Acciones Editar Vista Ayuda
(root@kali)-[~]
# sudo groupadd centro
(root@kali)-[~]
# sudo groupadd florida
(root@kali)-[~]
# sudo groupadd Giron
(root@kali)-[~]
# sudo groupadd Lulo
(root@kali)-[~]
# sudo groupadd tia
(root@kali)-[~]
# cat /etc/group

```

Se crean los respectivos grupos



```

centro:x:1001:
florida:x:1002:
Giron:x:1003:
Lulo:x:1004:
tia:x:1005:

```

Se verifica que los grupos se hayan creado

4. El señor Lulo le pide:
 - 4.1 Que cree un usuario para él.
 - 4.2 Que le cree un usuario a su tía.
 - 4.3 Que le cree un usuario al admin de la sede Centro.
 - 4.4 Que le cree un usuario al admin de la sede de Florida.
 - 4.5 Que le cree un usuario al admin de la sede de Girón.

```

root@kali: ~
Archivo Acciones Editar Vista Ayuda

(root@kali)-[~]
# sudo adduser lulito

Añadiendo el usuario `lulito' ...
Añadiendo el nuevo grupo `lulito' (1006) ...
Adding new user `lulito' (1006) with group `lulito (1006)' ...
Creando el directorio personal `/home/lulito' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
Las contraseñas no coinciden.
passwd: Error de manipulación del testigo de autenticación
passwd: no se ha cambiado la contraseña
¿Intentar de nuevo? [s/N] n
Cambiando la información de usuario para lulito
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
Nombre completo []: lulito jefe
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] s
Adding new user `lulito' to supplemental / extra groups `users' ...
Añadiendo al usuario `lulito' al grupo `users' ...

(root@kali)-[~]

```

```

gophish
lulito
admintia
admincentro
adminflorida
admingiron

```

Se verifica que se han creado los usuarios

```
centro:x:1001:admincentro
florida:x:1002:adminflorida
Giron:x:1003:admingiron
Lulo:x:1004:lulito
tía:x:1005:admintia
```

Se asignan los usuarios

5. Dentro del usuario del señor Lulo, debe crear un archivo llamado **compras**, este archivo debe tener los permisos de lectura y escritura activos para su propietaria, solo lectura para el grupo y ningún permiso para los otros. Dentro de este archivo, con el editor de su preferencia, escriba lo siguiente:

Vegetales

- ☐ Ajo
- ☐ Brocoli
- ☐ Cebolla
- ☐ Lechuga
- ☐ Papas
- ☐ Pepino
- ☐ Pimientos
- ☐ Repollo
- ☐ Tomates
- ☐ Zanahoria

```
(lulito@kali)-[~]
$ ls -lt
total 4
-rw-r--r-- 1 lulito lulito 44 ago 11 10:58 compras

(lulito@kali)-[~]
$ chmod 640 compras
```

Se creo el archivo y se asignó los permisos necesarios

6. En todos los demás usuarios cree un archivo llamado **ventas por sede**, el propietario de ese archivo debe ser root. Debe tener los permisos para el propietario, lectura y escritura para los otros y solo lectura para el grupo.

```
(root@kali)-[/home/admincentro]
# ls -l
total 0
-rw-r--r-- 1 root root 0 ago 11 11:07 ventas_por_sede
```

7. El joven Lulo le pide a usted que por favor al usuario del admin del Centro y de Florida no le deje ningún permiso activo sobre el archivo "**balance del día**".

```
(root@kali)-[~]
# sudo touch /balancedia.txt

(root@kali)-[~]
# sudo chmod 600 /balancedia.txt
```

```
(root@kali)-[/]
# ls -l /balancedia.txt

-rw----- 1 root root 0 ago 11 11:26 /balancedia.txt
```

Aquí se aplica la política de Zero Trust la cual se excluye todos los usuarios (Menos el root) debido a que se expone información sensible respecto a las ganancias del negocio.

8. Haga un listado de las contraseñas que asignó a cada uno de los usuarios que creó, describa cuál fue su política de contraseñas. ¿Dónde se guardan las contraseñas cifradas en el sistema de archivos de Linux?

```
shandels:$y$j9T$o/AEtvRfQAWJHl4REnf05.$fHjRuvxPiTvlbmiAxGMLf9ViT.50nCwkGA2Ib9
bk14/:19572:0:99999:7:::
_gophish!:19574:0:99999:7:::
lulito!:19580:0:99999:7:::
admintia:$y$j9T$K25ATSKS0RkiQINqddxVo/$nLyOhSMmQCVv9FszKcVlc3L1lfhLm1Eci5BgL
drex.:19580:0:99999:7:::
admincentro:$y$j9T$QKGUquyK7pz0IgDuQnObT0$3qhcaInRXZfNTgNg1Z8Tmzd2KoqNJLp8Jo/
PUapOPqD:19580:0:99999:7:::
adminflorida:$y$j9T$DY8c1wpwQ3s5ulFtbsuGC.$xW95bjcj4JgYuqH1W13F3Z3ACaSz3r3Q/8
lQ34D30r2:19580:0:99999:7:::
admingiron:$y$j9T$gnyD2*3afqpT64iAwmqbn.$gCUP4wwMccVGXngTCxvGNoCAFUi/.BeS000j
KJQZaE8:19580:0:99999:7:::
```

9. Escoja un gestor de contraseñas (tal como last pass), averigüe su valor y sus características, describa porqué lo escogió como el gestor de contraseñas que le va a pedir a Lulo que compre para gestionar las contraseñas de la organización.

- Bóveda segura: LastPass utiliza encriptación de grado militar para proteger las contraseñas y otros datos confidenciales. Los datos se cifran y descifran localmente en su dispositivo, y solo los datos cifrados se almacenan en los servidores de LastPass.
- Generador de contraseñas seguras: LastPass puede generar contraseñas únicas y seguras para cada sitio web y servicio, lo que ayuda a proteger su cuenta de ataques de fuerza bruta.

- Autenticación de dos factores (2FA): LastPass admite la autenticación de dos factores para agregar una capa adicional de seguridad a su cuenta. Puede usar aplicaciones de autenticación o dispositivos USB para mejorar la seguridad de su cuenta.
 - Autocompletar contraseña: LastPass puede completar automáticamente los campos de inicio de sesión en los sitios web, lo que facilita el acceso a su cuenta sin tener que recordar o ingresar una contraseña. Mantenga sus notas y datos seguros: además de las contraseñas, LastPass le permite almacenar de forma segura notas, números de tarjetas de crédito y otra información confidencial.
 - Acceso multiplataforma: LastPass está disponible en múltiples plataformas, incluidos navegadores web, aplicaciones móviles y extensiones para sistemas operativos como Kali Linux. Sincronización: puede sincronizar contraseñas y datos entre dispositivos para garantizar la coherencia en todos sus dispositivos.
 - Comprobador de seguridad: LastPass proporciona una evaluación de la seguridad de la contraseña y busca contraseñas débiles o duplicadas.
10. Cambie la contraseña para el usuario de Lulo, él le pide que lo haga porque la olvidó. ¿Se conservan los archivos asociados a la carpeta/directorio del usuario de Lulo si se cambia la contraseña?

```

root@kali: /
Archivo Acciones Editar Vista Ayuda
(root@kali)-[/]
# sudo passwd lulito
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
  
```

Cambiar la contraseña de un usuario no debería alterar los permisos ni la propiedad de esta carpeta, por lo que los archivos deberían permanecer intactos.

11. Lea el siguiente artículo y escoja al menos 3 comandos de los descritos en la lectura para explicarlo a sus compañeros, elabora una pequeña presentación de máximo 3 diapositivas para ello.

[11 comandos útiles en Linux si trabajas en seguridad \(welivesecurity.com\)](https://www.welivesecurity.com/2017/05/11/11-linux-commands-for-security/)