Soluciones examen seguridad

Ejercicio 1

1. Instalación de GPG (si es necesario)

```
sudo apt-get install gnupg
```

2. Generar la pareja de claves

```
gpg --full-generate-key
```

3. Guardar el mensaje cifrado y descifrarlo

```
echo "KEyC1rp1TOs1m3tRl1c@" > mensaje.asc
gpg --decrypt mensaje.asc
```

4. Crear el archivo de texto con la respuesta

```
echo "Tu nombre y apellidos y la respuesta al reto" > respuesta.txt
```

5. Cifrar el archivo de texto con la clave pública descifrada

```
gpg --encrypt --recipient <clave_publica_descifrada> respuesta.txt
```

6. Cifrar el archivo cifrado con tu propia clave pública

```
gpg --encrypt --recipient tu_email@example.com --output respuesta_final.txt.gpg
respuesta.txt.gpg
```

7. Firmar el archivo final cifrado con tu clave privada

```
gpg --sign --output respuesta_firmada.txt.gpg respuesta_final.txt.gpg
```

8. Exportar tu clave pública

```
gpg --export --armor tu_email@example.com > clave_publica.asc
```

9. Renombrar los archivos

```
mv respuesta_firmada.txt.gpg asir_apellido_nombre_sad_p1-mrz_respuesta.asc
mv clave_publica.asc asir_apellido_nombre_sad_p1-mrz_clave.asc
```

Ejercicio 2

1. **Preparar los discos virtuales**:
   - Discos utilizados: `/dev/sdb`, `/dev/sdc`, y `/dev/sdd`.
2. **Borrar el superblock de los discos**:

```
   sudo mdadm --zero-superblock /dev/sdb
   sudo mdadm --zero-superblock /dev/sdc
   sudo mdadm --zero-superblock /dev/sdd
```

3. **Crear el RAID 5**

```
sudo mdadm --create --verbose /dev/md0 --level=5 --raid-devices=3 /dev/sdb
/dev/sdc /dev/sdd
```

4. **Crear un sistema de archivos en el dispositivo RAID:**

```
sudo mkfs.ext4 /dev/md0
```

5. **Montar el dispositivo RAID:**

```
sudo mkdir -p /mnt/raid5
sudo mount /dev/md0 /mnt/raid5
```

6. **Verificar la configuración**

```
cat /proc/mdstat
```

7. **Crear el fichero de 10MB en el RAID:**

```
sudo dd if=/dev/zero of=/mnt/raid5/fichero_10MB bs=1M count=10
```

8. **Mostrar la estructura de los discos y el contenido del RAID:**

```
ls -lh /mnt/raid5/
lsblk -l
```

Ejercicio 3

1. **Descargar Nessus**

```
wget https://www.tenable.com/downloads/nessus
```

2. **Instalar Nessus**

```
sudo dpkg -i Nessus-<version>.deb
```

3. **Iniciar el Servicio de Nessus**

```
sudo systemctl start nessusd
```

4. **Acceder a la Interfaz Web de Nessus**

Abre un navegador y ve a https://<Kali_IP>:8834 (donde <Kali_IP> es la IP de tu máquina Kali, en este caso 192.168.2.10).

5. **Configurar Nessus**

Sigue las instrucciones en la interfaz web para completar la configuración inicial de Nessus y activar tu licencia

6. **Realizar el Escaneo de Vulnerabilidades**

6.1 **Crear un Nuevo Escaneo**

- Accede a la interfaz de Nessus.
- Crea una nueva política de escaneo o usa una política existente.
- Configura un nuevo escaneo con los siguientes detalles:
- Nombre del Escaneo: Análisis de Red Red_LAB_SAD
- Rango de IPs a Escanear: 192.168.2.0/27 (esto cubre hasta 30 nodos).

6.2 **Ejecutar el escaneo**

- Iniciar el escaneo

7. **Analisis de resultados**

- Exportar el informe
- Analizar las vulnerabilidades
    - Vulnerabilidades descubiertas
    - Relación de vulnerabilidades con servicios y puertos "well-know"
    - Medidas propuestas para solucionar las vulnerabilidades críticas