PRÁCTICA 1.7

Seguridad Informática y Normativa Legal

1. **Pon un ejemplo de medida de seguridad informática que sea:**
   - Física y pasiva:
   - Física y activa:
   - Lógica y pasiva:
   - Lógica y activa:

2. **Explica brevemente qué es y cómo funciona un sistema de alimentación ininterrumpida (SAI o UPS). Indica la diferencia entre las distintas topologías de SAI existentes (off-line, de linea interactiva y on-line). Busca en alguna tienda de informática un SAI indicando precio y las características que consideres de interés.**

3. **En cuanto a los discos duros redundantes, completa la siguiente tabla resumen:**

	N.º de discos	Tolerancia a fallos	Capacidad final
RAID 0			
RAID 1			
RAID 0+1			
RAID 5			
RAID 6			

4. **Vamos a crear un RAID 1 por software en la máquina virtual de Ubuntu instalada en la práctica anterior.**
   a) Con la máquina virtual apagada instalamos 2 discos duros nuevos, en "Configuración → Almacenamiento" añade dos discos nuevos de expansión dinámica de 10 GB cada uno, llamados "disco1" y "disco2" al controlador SATA.
   b) Inicia el sistema y comprueba los discos con el comando *" lsblk "*.
   c) Crea un directorio llamado RAID en /mnt ejecutando "*sudo mkdir /mnt/RAID*".
   d) Instala "mdadm" ejecutando en un terminal "*sudo apt update*" y "*sudo apt install mdadm*".

e) Crea un RAID 1 con los 2 discos nuevos con el comando *"sudo mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 /dev/sdb /dev/sdc"*

f) Comprueba la creación del RAID ejecutando "watch cat /proc/mdstat" hasta que el raid esté activo (sal con ctrl+c).

g) Crea un sistema de ficheros para el RAID "sudo mkfs.ext4 -F /dev/md0"

h) Edita /etc/fstab para que monte automáticamente durante el arranque el RAID ejecutando "sudo gedit /etc/fstab" añade la siguiente línea al final del fichero "/dev/md0 /mnt/RAID ext4 defaults,nofail 0 0".

i) Guarda la configuración del RAID con el siguiente comando: "sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf"

j) Actualiza el sistema de ficheros RAM inicial para que el RAID esté disponible durante el arranque: *"sudo update-initramfs -u"*

k) *Reinicia el sistema.*

l) Obtén una captura de pantalla del resultado de ejecutar el comando "sudo mdadm --detail /dev/md0"

m) Comprueba el espacio disponible en /mnt/RAID con *"df -h"*

n) Permite que todos puedan acceder al RAID ejecutando "*sudo chmod 777 /mnt/RAID*"

o) Crea un fichero de texto dentro de /mnt/RAID/ llamado "importante.txt" que contenga el texto "Fichero importante en el RAID "

5. Vamos a suponer que un disco del RAID ha fallado y que lo tenemos que sustituir por otro. Con la máquina virtual apagada desconecta el disco "disco2" e inicia el sistema.

a) Comprueba que no hay ficheros en /mnt/RAID/. ¿Qué información muestra "cat /proc/mdstat"?

b) Para el RAID "sudo mdadm --stop /dev/md0"

c) Ensambla el RAID con "sudo mdadm --assemble --scan" y comprueba que tienes acceso a los ficheros de /mnt/RAID. Ahora el RAID está funcionando con 1 solo disco.

d) Para la máquina virtual y añade otro disco llamado "reemplazo".

e) Añade al raid el nuevo disco con "sudo mdadm /dev/md0 -a /dev/sdc"

f) Comprueba que finaliza la recuperación ejecutando "cat /proc/mdstat"

g) Obtén una captura de pantalla del comando "sudo mdadm --detail /dev/md0"

6. **Instala grsync en la máquina virtual "sudo apt install grsync" y realiza las siguientes tareas:**
   - Crea 5 ficheros dentro de Documentos llamados doc1, doc2, doc3, doc4 y doc5.
   - Configura grsync para sincronizar el directorio "Documentos" con "/mnt/RAID" y realiza una sincronización.
   - Modifica el contenido de doc3 y elimina doc5.
   - Realiza otra sincronización y visualiza qué ficheros se han copiado viendo la "Salida de rsync".
   - ¿Qué tipos de copia se están realizando?

7. **Analiza en www.virustotal.com algún fichero ejecutable que tengas, el fichero "virus.zip" y alguna URL que consideres sospechosa. Obtén capturas de pantalla del resultado de los análisis. Analiza ahora "virus.zip.tgz.tgz", ¿que explicación tienen estos últimos resultados?.**

8. **Indica brevemente la diferencia entre troyano, spyware y ransomware.**

9. **Vamos a probar el cifrado simétrico con gpg:**
   - Crea un documento de texto con cualquier editor.
   - Cifra este documento con alguna contraseña *"gpg -c documento.txt"*
   - Haz llegar por algún medio a algún compañero el documento que acabas de cifrar (documento.txt.gpg).
   - Descifra el documento que te ha hecho llegar algún compañero.
   - Repite el proceso anterior con otro documento de texto, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.
   - Copia y pega el contenido del archivo cifrado anteriormente y envíalo por email a algún compañero para que lo descifre.
   - Descifra el contenido del email cifrado recibido.
   - ¿Cómo has proporcionado tu clave de cifrado al compañero? ¿Cuál es el punto más débil del cifrado simétrico?

10. Vamos a probar el cifrado asimétrico con gpg:

- Crea tu par de claves pública y privada. Tipo de cifrado 1 (RSA), tamaño 1024 y validez de 1 mes *"gpg --gen-key".*
- Lista tus claves "*gpg --list-keys"*
- Exporta tu clave pública en un archivo *nombre_apellido.asc* y envíalo a varios compañeros *"gpg --export -a "Nombre Apellidos" > nombre_apellido.asc"*
- Importa las claves públicas recibidas de tus compañeros *"gpg --import clave_publica_recibida.asc".*
- Comprueba que las claves se han incluido correctamente volviendo a listar las claves.
- Cifraremos un archivo cualquiera y lo remitiremos por email a algunos de los compañeros que nos proporcionó su clave pública *"gpg -a -r Compañero1 -r Compañero2 --encrypt documento.txt".*
- Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos *"gpg documento_cifrado.asc".*
- Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar el archivo.
- ¿Qué clave se usa para cifrar, la pública o la privada?

11. Firma digital de un documento con gpg:

- Crea la firma digital de un archivo de texto cualquiera y envía la firma junto al documento a un compañero *"gpg --output firma_documento.txt.sig --detach-sign documento.txt".*
- Verifica que la firma recibida del documento es correcta *"gpg --verify firma_documento.txt.sig documento.txt".*
- Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.
- Realiza un cifrado con firma para un documento *"gpg --output documento2.txt.sig --sign documento2.txt".*
- Envía *documento2.txt.sig* a algún compañero, verifica la firma y descifra el fichero.
- ¿Qué clave se usa para firmar, la pública o la privada?

12. **Accede a la página web del Instituto Nacional de Seguridad (INCIBE):** https://www.incibe.es/protege-tu-empresa/que-te-interesa **consultando el dosier que se indica entre paréntesis si fuera necesario**

    a) ¿Qué debemos hacer con el desechado y reutilización de soportes y equipos que almacenan información? (Protección de la información)

    b) ¿Qué medidas de seguridad son las recomendadas en el uso de redes wifi propias o de terceros? (Protección en movilidad y redes inalámbricas.)

    c) ¿Qué información debe aparecer como mínimo en una página web si vendemos servicios a través de Internet? (Protege tu web.)

    d) ¿Qué leyes relacionadas con la seguridad deben cumplir pymes y autónomos? (Cumplimiento legal.)

    e) ¿Qué información se recomienda que tenga el etiquetado e inventario de los soportes móviles de una empresa? (Buenas prácticas en el área de la informática.)

13. **He desarrollado una aplicación para móvil y quiero registrarla con copyright, indica que puedo hacer y que coste tiene. Al final me he decidido por publicarla como software libre con licencia GPL, explica cuales son las 4 libertades del software libre y en qué consiste la licencia GPL.**

Nota: *La práctica se entregará en el aula virtual en formato pdf indicando en el fichero el número de práctica y tu nombre con el siguiente formato: prácticaX.X_nombre.pdf*