

Nombre del Alumno: Belén Nazareth Durán Meléndez

Calificación:

Parte I

Parte II

Parte III

PARTE I (Seguridad):

1. ¿Tienes ordenador en casa? ¿Lo usas solo tú? ¿Qué características principales tiene?
Actualmente sólo hay un ordenador, lo uso solo yo y de características principales:
cuenta con 18GB de RAM, 512GB de almacenamiento y ryzen 5.

2. Explica qué es para ti el concepto de Seguridad Informática.
Seguridad informática es igual al método compuesto de diferentes técnicas usado para proteger los dispositivos de ataques externos, aunque también puede ser las diferentes medidas que tomamos durante el uso de los dispositivos como puede ser evitar el autoguardado de contraseñas, el uso de diferentes contraseñas o tener en cuenta y observar bien la seguridad de las páginas en las que se entran.

3. ¿Qué es un hacker ético?
En mi opinión es aquel que coge tus datos a partir de un acuerdo donde aceptas los términos de uso de tus datos.

4. ¿Sabes qué es la criptografía? Pon un ejemplo de uso.
Creo que la criptografía es el método usado para proteger datos almacenados en un dispositivo.

5. Explica a continuación para qué crees que sirven los siguientes dispositivos:

- Cortafuegos

- VPN

- SAI

6. ¿Qué es un sistema biométrico?
Es un sistema de seguridad en el que en lugar de usar una contraseña o pin se usa la huella dactilar o el reconocimiento facial entre otros.

7. ¿Qué son los metadatos de un fichero?
Son los datos que componen ese fichero.

8. ¿Qué es el malware?

9. ¿Conoces alguna forma de aprender ciberseguridad de forma gratuita?

Mediante cursos online gratuitos, eventos online en directo en redes sociales, videos de creadores de contenido de youtube, tiktok o instagram, páginas web o en la biblioteca, en foros...

10. Explica los siguientes términos:

- Pentesting
- Informática Forense
- CTF
- Escalado de privilegios

PARTE II. SSOO:

1. ¿Cómo encontrarías un fichero en Linux desde línea de comandos?

2. ¿Cómo montarías varias particiones en un mismo disco en Linux desde línea de comandos? Explícalo detalladamente.

Primero se define la partición y después usando el comando mount seguido de la partición.

3. ¿Cómo encontrarías una cadena concreta dentro de un fichero usando la línea de comandos de Linux?

Con una expresión regular ya sea grep o egrep.

4. ¿Has realizado alguna vez una copia de seguridad? ¿Con qué sistema o herramientas?

Si, usando un snapshot.

5. ¿Para qué sirve en Linux el operador &&? ¿Y &? ¿Y el >>?

&&: para concatenar comandos de tal manera que una vez se realice el primero, si sale bien siga con el siguiente comando.

&: para que se realice primero un comando y seguido el siguiente comando.

»: para redireccionar datos a una fichero sin sobrescribir, se van colocando los datos en la ultima linea del fichero.

6. ¿Qué permiten los permisos 754 en un fichero?

Permiten leer, escribir y ejecutar al usuario, leer y ejecutar a grupos y otros.

7. ¿Dónde se encuentran habitualmente los ficheros de log en Linux?

8. ¿Qué editor de texto usas desde línea de comandos habitualmente?

Vim y nano.

9. ¿Para qué sirve el comando scp?

Sirve para copiar ficheros mediante ssh.

10. ¿Qué comando usarías para saber los procesos que se están ejecutando en tu máquina Linux?

Htop o top

PARTE III. Redes:

1. ¿Cómo podemos saber los puertos que se están usando en nuestro ordenador?

2. ¿Qué diferencia hay entre TCP y UDP? ¿Para qué suele usarse cada uno de ellos?

3. Explica qué se añade a un mensaje en la cabecera de nivel de enlace. ¿Y en la de nivel de red? ¿Y en la de nivel de transporte?

4. En los distintos saltos de un router a otro que puede dar un mensaje, ¿cambian las direcciones MAC de origen y destino o las direcciones IP de origen y destino? Explica el motivo.

Cambian las direcciones ip dependiendo de si es publica o privada y de la ip base que tenga esa red.

5. ¿Qué es SNAT y DNAT?

SNAT: Es el cambio de la ip de red privada a publica.

DNAT: Es el cambio de la ip de red publica a privada.

6. ¿Para qué sirve el DNS?

Para traducir los dominios a ip.

7. ¿Qué es el protocolo ARP?

Es el protocolo encargado de enviar datos en paquetes.

8. Si una tarjeta de red tiene la dirección 169.254.1.1. ¿Qué puede estar pasando?

9. ¿Dónde se encuentra en Linux el fichero de configuración de la tarjeta de red?

10. Explica la función de los siguientes comandos:

- nslookup

Buscar la ip de un dispositivo.

- dig

Para buscar el DNS de un servidor.

- traceroute

Para ver como los paquetes pasan por internet.

- wget

Para obtener recursos a traves de un enlace.