Apellidos: _____

Nombre: _____

Fecha: _____ **Grupo:** _____

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	

Instrucciones generales para las preguntas cerradas:

- No se tendrán en cuenta anotaciones fuera de la tabla de respuestas.
- Todas las preguntas tienen el mismo valor.
- Hay una, y sólo una, respuesta correcta en cada pregunta.
- Responde solo a aquellas preguntas de las que estés seguro. Una respuesta incorrecta resta un tercio del valor de una respuesta acertada, pero una pregunta sin responder no resta puntos.
- Escribe la respuesta con letras MAYÚSCULAS. Para cambiar la respuesta, tacha y escribe la nueva respuesta.

Instrucciones generales para las preguntas abiertas:

- Es necesario responder a la pregunta y justificar dicha respuesta.
- Todas las preguntas tienen el mismo valor.

Puntuación:

- La parte tipo test es un 60 % de la nota.
- La parte de preguntas abiertas es un 40 % de la nota.
- Se necesita un mínimo de 3,5 en cada parte del examen para que hagan media.

1. En un ordenador PC típico, pueden protegerse por contraseña

a) El sistema operativo, la BIOS y el cargador del sistema operativo (GRUB)

b) El sistema operativo, la BIOS, el cargador del sistema operativo (GRUB) y los dispositivos

c) La BIOS y el sistema operativo

d) El sistema operativo, la BIOS, el cargador del sistema operativo (GRUB) y los discos

2. Las listas de control de acceso

a) Especifican los recursos a los que tiene acceso un usuario

b) Especifican las contraseñas necesarias para acceder a un recurso

c) Pueden especificar quién tiene un permiso concedido para acceder a un recurso, pero también quién tiene ese permiso denegado

d) Especifican quién tiene concedido un permiso

3. Un sistema operativo aplica control de acceso

a) Cada vez que un proceso accede a algún recurso con ACL

b) Cuando el usuario hace "login" y cada vez que un proceso accede a un fichero/dispositivo

c) Cuando el usuario hace "login"

d) Cuando un proceso accede a un fichero/dispositivo

4. ¿Por qué se necesitan números aleatorios al generar una clave asimétrica?

a) Para que la clave tenga más bits de longitud

b) Para captar las características biométricas del usario que la genera

c) Para que un atacante no pueda reproducir el proceso de generación de la clave, y así conseguir dicha clave

d) Para asegurar que la clave es más asimétrica que simétrica

5. El permiso "s" de UNIX/Linux

a) Hace que un fichero ejecutable tenga que ser lanzado mediante "sudo"

b) Hace que un fichero ejecutable se ejecute siempre con los permisos del usuario que lo ejecuta

c) Hace que un fichero ejecutable se ejecute siempre con los permisos del usuario propietario del fichero

d) Hace que un fichero ejecutable no pueda ser lanzado mediante "sudo"

6. El comando "sudo" se utiliza en lugar del usuario "root" porque

a) Se consigue que varios usuarios puedan administrar el equipo sin poder cambiar la contraseña de "root"

b) No hay usuario root en los sistemas que tienen "sudo"

c) Hay ciertas tareas que ni siquiera el usuario "root" puede realizar, a no ser que sea a través de "sudo"

d) Se consigue que varios usuarios puedan administrar el equipo sin conocer la contraseña de root

7. Encriptando los datos de los discos puede conseguirse

a) Que no se puedan modificar los datos, a no ser que se posea la contraseña de GRUB

b) Que no se pueda acceder a los datos, a no ser que se tenga acceso físico al sistema

c) Que no se puedan modificar los datos, a no ser que se posea la contraseña de la BIOS

d) Que no se pueda acceder a los datos ni siquiera con acceso físico al sistema

8. La seguridad biométrica

a) Es la seguridad basada en la contraseña de la BIOS

b) Es la autentificación basada en características personales

c) Es la autentificación basada en datos personales (como la LOPD)

d) Es la encriptación mediante passphrase, no mediante password

9. Si un límite de un sistema de cuotas es "blando"

a) Es un límite grande, de forma que no afecte mucho al usuario que lo tiene

b) Es el límite que puede sobrepasarse, y al hacerlo se recibe algún tipo de aviso

c) Es un límite pequeño, de forma que no afecte mucho a los otros usuarios

d) Es un límite que no puede sobrepasarse, pero se recibe un aviso antes de llegar a él

10. La diferencia entre el usuario Administrador de Windows y root de Linux reside en que

a) El usuario Administrador puede hacer cualquier cosa, y el root tiene algunas limitaciones

b) El usuario Administrador no se puede deshabilitar, pero el usuario root sí

c) El usuario root puede hacer cualquier cosa, y el Administrador tiene algunas limitaciones

d) Simplemente, uno es de Windows y otro de Linux

11. Los registros de monitorización en Windows

a) Se consultan en el directorio C:\windows\system\drivers\var\log

b) Se consultan en el registro de windows (con regedit32)

c) Se consultan en el visor de sucesos (event viewer)

d) Se consultan en el directorio C:\windows\log

12. Los registros de monitorización en Ubuntu Linux

a) Se consultan en el fichero /var/log

b) Se consultan con el comando tail

c) Se consultan con el comando eview

d) Se consultan en el directorio /var/log

13. Las BIOS tienen

a) Como mucho, una contraseña para usar el ordenador
b) Pueden tener una contraseña para modificar los datos de la BIOS, y otra para usar el ordenador
c) Como mucho, una contraseña para modificar los datos de la BIOS
d) Pueden tener una contraseña para modificar la BIOS y otra por cada sistema operativo instalado

14. Cuando no se guarda la contraseña directamente, sino su hash (resumen), se hace

a) Porque el hash se encripta con la clave de root (o administrador), y así solamente él puede conocer las contraseñas de los usuarios
b) Para que no se conozca el nombre de usuario asociado a la contraseña
c) Para ahorrar tiempo en el paso de calcular el hash cuando haya que compararlo con el de la contraseña introducida
d) Porque no es fácil encontrar otra contraseña que de el mismo valor de hash

15. Las cuotas de disco mejoran

a) La integridad
b) La disponibilidad
c) El no repudio
d) La confidencialidad

16. Las cuotas de disco no tienen efecto

a) Si el límite soft (blando) es distinto al límite hard (duro)
b) Si el límite que imponen es superior al tamaño del disco
c) Si el límite que imponen es inferior al tamaño del disco
d) Si el límite soft (blando) es inferior al límite hard (duro)

17. El uso de VLANS en una red local mejora

a) La disponibilidad y el no repudio
b) El no repudio
c) No mejora ninguna característica segura, solo la velocidad
d) La confidencialidad

18. Los sistemas de encriptación más comunes de las redes wifi son

a) WEP y PSK
b) Radius y PSK
c) WPA y WEP
d) Radius y WPA

19. Un servidor RADIUS

a) Realiza la autentificación, basada en usuario y contraseña
b) Realiza la encriptación, basada en usuario y contraseña
c) Realiza la autentificación, basada en una lista de direcciones MAC
d) Realiza la encriptación, basada en una lista de direcciones MAC

20. Es preferible usar WEP sobre WPA cuando

a) Los equipos tienen mucha potencia de cálculo, y se busca seguridad
b) Se quiere autentificar a los usuarios, pero sin cifrar la información
c) Los equipos no tienen mucha potencia de cálculo, y se busca velocidad
d) Se quiere autentificar a los usuarios, además de cifrar la información

21. Elige la opción correcta acerca de las redes WiFi

a) WPA2 utiliza RC4 para encriptar
b) WEB utiliza AES para encriptar
c) WEP utiliza RC4 para encriptar
d) WPA2 utiliza AES para identificar a cada usuario, porque cada uno puede tener su propia contraseña

22. Los siguientes protocolos pueden usarse para establecer una VPN

a) IPSec, AES y RADIUS
b) AES y L2TP
c) IPSec y L2TP
d) PPTP y RADIUS

23. ¿Qué protocolo de VPN es más seguro?

a) IPSec es más seguro de AES
b) L2TP es más seguro que PPTP
c) PPTP es más seguro que RADIUS
d) PPTP es más seguro que L2TP

24. Un proxy es un elemento de interconexión que entiende los protocolos

a) Hasta el nivel de enlace
b) Hasta el nivel de red, o incluso capas más bajas
c) Hasta el nivel de transporte, o incluso capas más altas
d) Hasta el nivel de red

25. Describe la secuencia de arranque de un PC, identificando los momentos en los que típicamente puede solicitarse una contraseña

26. Explica por qué los proxy-caché pierden su eficacia si se utilizan con un protocolo sobre SSL/TLS

27. Explica por qué NAT se utiliza como firewall

28. Realiza un diagrama de la red de una empresa en la que se ha instalado una DMZ con doble firewall. La empresa tiene 4 puestos utilizados como workstation, y pretende ofrecer a los usuarios de Internet un servicio Web y uno de DNS