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 quién tiene concedido un permiso
   b) Pueden especificar quién tiene un permiso concedido para acceder a un recurso, pero también quién tiene ese permiso denegado
   c) Especifican las contraseñas necesarias para acceder a un recurso
   d) Especifican los recursos a los que tiene acceso un usuario

3. Un sistema operativo aplica control de acceso
   a) Cuando un proceso accede a un fichero/dispositivo
   b) Cuando el usuario hace "login" y cada vez que un proceso accede a un fichero/dispositivo
   c) Cada vez que un proceso accede a algún recurso con ACL
   d) Cuando el usuario hace "login"

4. ¿Por qué se necesitan números aleatorios al generar una clave asimétrica?
   a) Para asegurar que la clave es más asimétrica que simétrica
   b) Para que un atacante no pueda reproducir el proceso de generación de la clave, y así conseguir dicha clave
   c) Para captar las características biométricas del usario que la genera
   d) Para que la clave tenga más bits de longitud

5. El permiso "s" de UNIX/Linux
   a) Hace que un fichero ejecutable no pueda ser lanzado mediante "sudo"
   b) Hace que un fichero ejecutable se ejecute siempre con los permisos del usuario propietario del fichero
   c) Hace que un fichero ejecutable se ejecute siempre con los permisos del usuario que lo ejecuta
   d) Hace que un fichero ejecutable tenga que ser lanzado mediante "sudo"

6. El comando "sudo" se utiliza en lugar del usuario "root" porque
   a) Hay ciertas tareas que ni siquiera el usuario "root" puede realizar, a no ser que sea a través de "sudo"
   b) Se consigue que varios usuarios puedan administrar el equipo sin poder cambiar la contraseña de "root"
   c) Se consigue que varios usuarios puedan administrar el equipo sin conocer la contraseña de root
   d) No hay usuario root en los sistemas que tienen "sudo"

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 la BIOS
   b) Que no se pueda acceder a los datos, a no ser que se tenga acceso físico al sistema
   c) Que no se pueda acceder a los datos ni siquiera con acceso físico al sistema
   d) Que no se puedan modificar los datos, a no ser que se posea la contraseña de GRUB

8. La seguridad biométrica
   a) Es la seguridad basada en la contraseña de la BIOS
   b) Es la autentificación basada en datos personales (como la LOPD)
   c) Es la encriptación mediante passphrase, no mediante password
   d) Es la autentificación basada en características personales

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 root puede hacer cualquier cosa, y el Administrador tiene algunas limitaciones
   c) El usuario Administrador no se puede deshabilitar, pero el usuario root sí
   d) Simplemente, uno es de Windows y otro de Linux

11. Los registros de monitorización en Windows
   a) Se consultan en el visor de sucesos (event viewer)
   b) Se consultan en el directorio C:\windows\system\drivers\var\log
   c) Se consultan en el registro de windows (con regedit32)
   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 eview
   c) Se consultan en el directorio /var/log
   d) Se consultan con el comando tail

13. Las BIOS tienen

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

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

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

15. Las cuotas de disco mejoran

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

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 soft (blando) es inferior al límite hard (duro)
d) Si el límite que imponen es inferior al tamaño del disco

17. El uso de VLANS en una red local mejora

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

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

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

19. Un servidor RADIUS

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

20. Es preferible usar WEP sobre WPA cuando

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

21. Elige la opción correcta acerca de las redes WiFi

a) WEB utiliza AES para encriptar
b) WPA2 utiliza RC4 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) AES y L2TP
b) PPTP y RADIUS
c) IPSec y L2TP
d) IPSec, AES y RADIUS

23. ¿Qué protocolo de VPN es más seguro?

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

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

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

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