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		25	
26		27		28		29		30	
31		32							

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.
- Un aspa marca una respuesta. Se puede desmarcar una respuesta con un círculo sobre el aspa.

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. Una persona que extrae y analiza los datos que se transmiten por una línea de comunicación es un
   a) DoS
   b) Phreaker
   c) Hacker
   d) Sniffer

2. Un sistema capaz de detectar usuarios y contraseñas, ya sean contraseñas para el sistema local o para sistemas accedidos remotos, es un
   a) Sniffer
   b) Spoofing
   c) Phreaker
   d) Keylogger

3. El phishing
   a) No necesita sniffing, pero hace que sea mas eficaz
   b) Suele estar asociado a spam, pero podría realizarse por otros medios (por ejemplo, anuncios en periódicos)
   c) Necesita sniffing en todos los casos
   d) Implica siempre spam

4. Un adware
   a) Es indetectable por el usuario
   b) Es un virus, pero no un troyano
   c) Muestra mensajes al usuario
   d) Es un virus, del tipo troyano

5. Es spyware
   a) Todos los virus
   b) Todos los adware
   c) Todos los spoofing
   d) Todos los keyloggers

6. Un malware que modifica otros ficheros ejecutables para que contengan copias del malware es un
   a) Hoax
   b) Virus
   c) Troyano
   d) Adware

7. Un malware que se propaga, pero sin modificar otros ficheros ejecutables, es un
   a) Virus
   b) Gusano
   c) Troyano
   d) Hoax

8. El payload
   a) Es un sinónimo de spyware
   b) Es el sistema de propagación de un malware
   c) Es un sinónimo de adware
   d) Es la función maliciosa de un malware

9. La llamada a casa de un malware
   a) Se usa para instalar un rootkit
   b) Puede evitarse instalando un firewall con NAT
   c) Se usa para comunicar datos privados del usuario, o modificar el payload
   d) Se usa para infectar a nuevos sistemas

10. Un troyano se caracteriza porque
    a) El usuario colabora en su instalación en el sistema
    b) Roba contraseñas, especialmente de cuentas de banco
    c) Instala un keylogger
    d) Se instala a través de spam

11. La clasificación de los malwares (virus, ransomware, addware, gusano,...) se suele basar en
    a) Por su nivel de impacto en la seguridad
    b) Por su forma de propagación y las acciones de su payload
    c) Por el tipo de hacker que lo ha creado
    d) Por la forma en que se combate desde las políticas de seguridad

12. Un mensaje en el que se da una noticia impactante, pero de baja credibilidad, es un
    a) Hoax
    b) Troyano
    c) Spam
    d) Phishing

13. Las actualizaciones de software
    a) No son importantes para la seguridad, excepto la del antivirus
    b) Son importantes para la seguridad, ya que pueden arreglar vulnerabilidades
    c) No son importantes para la seguridad, pero sí para el usuario, ya que añaden nuevas funcionalidades
    d) Deben retrasarse lo más posible, porque son una fuente de troyanos (excepto la actualización del antivirus)

14. Las actividades del _____ se orientan a perjudicar al atacado, y a veces a obtener algún provecho de ello
    a) Cracker
    b) Samurai
    c) Hacker
    d) Nerd

15. Se llama poisoning, en ocasiones, al
    a) Phishing
    b) Fuerza bruta
    c) Spoofing
    d) Sniffing

16. Para conseguir un ataque man-in-the-middle, suele ser necesario utilizar previamente

a) Phishing
b) Denial of service
c) Fuerza bruta
d) Spoofing

17. Desde el punto de vista del atacante, un ataque de diccionario es una alternativa a

a) Denial of service
b) Fuerza bruta
c) Code injection
d) Flooding

18. El malware más complicado de detectar es

a) Un spam
b) Un rootkit
c) Un DOS
d) Un gusano

19. Un rootkit

a) Modifica el sistema operativo para ocultar la presencia del malware
b) Es un exploit para conseguir privilegios de administrador
c) Permite que el atacante se conecte a la máquina infectada
d) Se comunica con un servidor de internet, de forma que cede el control del sistema infectado al atacante

20. Una botnet

a) Es un conjunto de ordenadores ejecutando un antivirus que aisla una red interna de Internet
b) Es un conjunto de ordenadores protegidos por el mismo antivirus
c) Es un conjunto de ordenadores realizando un DoS
d) Es un conjunto de ordenadores infectados por un malware, y controlados por el atacante

21. Elige la política de contraseñas más segura (sin incluir la ñ)

a) Tres letras mayúsculas o minúsculas seguidas de tres números
b) 8 números
c) Cinco letras mayúsculas o minúsculas
d) Cuatro letras minúsculas seguidas de tres números

22. El antivirus puede ejecutarse

a) Al vuelo, a demanda, antes de la carga del sistema operativo y antes del arranque BIOS
b) A demanda
c) Al vuelo y a demanda
d) Al vuelo, a demanda y antes de la carga del sistema operativo

23. Al cifrar un texto en claro con una de las claves de un sistema asimétrico, el texto cifrado resultante

a) Es igual al texto cifrado que se conseguiría con la otra clave asimétrica
b) Tiene siempre la misma longitud (por ejemplo, 32 bytes para MD5)
c) Se puede descifrar con la otra clave del sistema asimétrica
d) Se puede descifrar con la misma clave del sistema asimétrico

24. Para mejorar el objetivo de "no repudio" de los envíos de información

a) Hay que enviar el fichero encriptado y sin encriptar, para su comparación
b) Basta con firmar los ficheros
c) Basta con encriptar los ficheros
d) Hay que firmar y encriptar los ficheros

25. En un sistema de clave simétrica

a) Es un problema el intercambio de claves, ya que si un tercero intercepta la clave puede cambiar las firmas electrónicas
b) No es posible realizar firma electrónica
c) No es posible desencriptar sin la clave privada
d) No es un problema el intercambio de claves, ya que si un tercero intercepta la clave no puede desencriptar los envíos

26. Para conseguir una firma electrónica se necesita

a) Una función resumen y un sistema de claves de tipo simétrico
b) Un canal seguro y un sistema de claves simétrico
c) Una función resumen y un sistema de claves de tipo asimétrico
d) Un canal seguro y un sistema de claves asimétrico

27. En un sistema de criptografía híbrida, como el estudiado en clase

a) Una de las partes inventa sobre la marcha un par de claves (pública y privada)
b) Una de las partes inventa sobre la marcha una clave pública
c) Una de las partes inventa sobre la marcha una clave privada
d) Una de las partes inventa sobre la marcha una clave simétrica

28. Las siglas PKI hacen referencia a

a) El conjunto de una clave pública y privada, empaquetadas en un certificado x509
b) El conjunto de certificados raíz de mi navegador web
c) El estándar que permite intercambiar claves públicas, y confiar en ellas
d) El programa que se suele utilizar para la criptografía de clave pública

29. El "Cifrado del César" es

a) Criptografía asimétrica, porque se usa distinto algoritmo para cifrar que para descifrar

b) Criptografía simétrica, porque se usa la misma clave para cifrar y descifrar

c) Criptografía estadística, porque se necesitan probar varias posibilidades

d) Criptografía híbrida, porque mezcla métodos manuales y automáticos

30. La autenticación consiste en

a) usar métodos biométricos

b) otorgar permisos a cierto usuario

c) firmar un documento

d) verificar la identidad de un usuario

31. Se dice de un certificado que es raíz si

a) Es un certificado considerado seguro, que puede firmar otros certificados

b) Es el certificado asociado a la raíz del DNS (.)

c) Es el certificado que se utilizó para instalar el sistema operativo

d) Es un certificado firmado por otro que tenga mayor nivel

32. En una comunicación HTTPS

a) El servidor podría requerir también un certificado del usuario, aunque no es común

b) Solo puede haber un certificado, que es el que el servidor envía al cliente

c) No hay certificados con claves públicas, ya que se usa criptografía asimétrica

d) No hay certificados con claves públicas, ya que se usa criptografía híbrida

33. Explica como un keygen (para instalar un programa sin licencia) puede utilizarse para distribuir malware

34. Describe en qué consiste un ataque de DHCP spoofing. Describe qué medidas pueden tomarse para evitar este tipo de ataques.

35. Describe cómo se realiza la comunicación utilizando criptografía híbrida (como en los protocolos SSL/TLS). Incluye un diagrama temporal como los utilizados en clase