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		

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

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

3. Cuando un servicio informático (por ejemplo, una web) es imitado por otro para hacerse pasar por el servicio original, se esta utilizando
   a) Spoofing
   b) Spamming
   c) Dos
   d) Phishing

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

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

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

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

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

9. La llamada a casa de un malware
   a) Puede evitarse instalando un firewall con NAT
   b) Se usa para instalar un rootkit
   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) Roba contraseñas, especialmente de cuentas de banco
   b) Se instala a través de spam
   c) Instala un keylogger
   d) El usuario colabora en su instalación en el sistema

11. La ingeniería social
   a) Se utiliza para hacer sniffing
   b) Consiste en manipular sistemas biométricos de autentificación
   c) Se basa en el comportamiento social usual de las personas
   d) Encuentra formas de construir contraseñas que las personas puedan recordar fácilmente

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

13. Las actualizaciones de software
   a) Son importantes para la seguridad, ya que pueden arreglar vulnerabilidades
   b) No son importantes para la seguridad, pero sí para el usuario, ya que añaden nuevas funcionalidades
   c) No son importantes para la seguridad, excepto la del antivirus
   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) Samurai
   b) Hacker
   c) Nerd
   d) Cracker

15. 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

16. Un rootkit

a) Permite que el atacante se conecte a la máquina infectada

b) Modifica el sistema operativo para ocultar la presencia del malware

c) Se comunica con un servidor de internet, de forma que cede el control del sistema infectado al atacante

d) Es un exploit para conseguir privilegios de administrador

17. 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

18. Los ataques de code injection se caracterizan por

a) Aprovechar vulnerabilidades de los programas o servicios para que ejecuten un código elegido por el atacante

b) Propagarse como un troyano

c) Propagarse como un gusano

d) Provocar una denegación de servicio (DOS)

19. El antivirus puede ejecutarse

a) Al vuelo y a demanda

b) A demanda

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

d) Al vuelo, a demanda y antes de la carga del sistema operativo

20. La criptografía híbrida

a) Mezcla encriptación y firma

b) Mezcla claves públicas y privadas

c) Mezcla métodos simétricos y asimétricos

d) Mezcla métodos de sustitución y transposición

21. 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 desencriptar sin la clave privada

c) No es un problema el intercambio de claves, ya que si un tercero intercepta la clave no puede desencriptar los envíos

d) No es posible realizar firma electrónica

22. Son funciones resumen

a) MD5, GPL

b) SHA1, PKI

c) PKI, MD5

d) MD5, SHA1

23. La desventaja de un sistema de clave asimétrica respecto de uno con clave simétrica es que

a) Es más lento, por el tiempo de proceso

b) Es menos seguro, porque es una tecnología más antigua

c) Es menos seguro, porque las claves son más cortas

d) Es menos seguro el intercambio de claves

24. En una comunicación se comienza utilizando una clave asimétrica para intercambiar una clave simétrica. Esto se hace para

a) Aumentar el objetivo de "no repudio"

b) Ahorrar tiempo de proceso, ya que las claves simétricas son más difíciles de computar

c) Ahorrar tiempo de proceso, ya que las claves asimétricas son más difíciles de computar

d) Aumentar la confidencialidad

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

a) Una de las partes inventa sobre la marcha una clave pública

b) Una de las partes inventa sobre la marcha un par de claves (pública y privada)

c) Una de las partes inventa sobre la marcha una clave simétrica

d) Una de las partes inventa sobre la marcha una clave privada

26. El "Cifrado del César" es

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

b) Criptografía estadística, porque se necesitan probar varias posibilidades

c) Criptografía híbrida, porque mezcla métodos manuales y automáticos

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

27. La autenticación consiste en

a) firmar un documento

b) verificar la identidad de un usuario

c) otorgar permisos a cierto usuario

d) usar métodos biométricos

28. En una comunicación HTTPS

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

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

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

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

29. Describe qué medidas pueden tomarse ante el phishing

30. Describe cómo se puede utilizar un sistema de criptografía asimétrica para realizar la firma digital de un fichero

31. Describe qué pasos realiza un navegador web para decidir que una conexión https es segura