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) 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) Phreaker
   b) Keylogger
   c) Sniffer
   d) Spoofing

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

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

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

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

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

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

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

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

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

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

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

15. Desde el punto de vista del atacante, un ataque de diccionario es una alternativa a
    a) Code injection
    b) Fuerza bruta
    c) Flooding
    d) Denial of service

16. Un rootkit

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

17. Una botnet

a) Es un conjunto de ordenadores protegidos por el mismo antivirus
b) Es un conjunto de ordenadores ejecutando un antivirus que aisla una red interna de Internet
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) Provocar una denegación de servicio (DOS)
b) Propagarse como un gusano
c) Aprovechar vulnerabilidades de los programas o servicios para que ejecuten un código elegido por el atacante
d) Propagarse como un troyano

19. El antivirus puede ejecutarse

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

20. La criptografía híbrida

a) Mezcla métodos simétricos y asimétricos
b) Mezcla claves públicas y privadas
c) Mezcla métodos de sustitución y transposición
d) Mezcla encriptación y firma

21. En un sistema de clave simétrica

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

22. Son funciones resumen

a) PKI, MD5
b) MD5, SHA1
c) MD5, GPL
d) SHA1, PKI

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

a) Es menos seguro, porque las claves son más cortas
b) Es menos seguro el intercambio de claves
c) Es menos seguro, porque es una tecnología más antigua
d) Es más lento, por el tiempo de proceso

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

a) Aumentar la confidencialidad
b) Aumentar el objetivo de "no repudio"
c) Ahorrar tiempo de proceso, ya que las claves simétricas son más difíciles de computar
d) Ahorrar tiempo de proceso, ya que las claves asimétricas son más difíciles de computar

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

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

26. El "Cifrado del César" es

a) Criptografía híbrida, porque mezcla métodos manuales y automáticos
b) Criptografía simétrica, porque se usa la misma clave para cifrar y descifrar
c) Criptografía estadística, porque se necesitan probar varias posibilidades
d) Criptografía asimétrica, porque se usa distinto algoritmo para cifrar que para descifrar

27. La autenticación consiste en

a) usar métodos biométricos
b) otorgar permisos a cierto usuario
c) verificar la identidad de un usuario
d) firmar un documento

28. En una comunicación HTTPS

a) No hay certificados con claves públicas, ya que se usa criptografía híbrida
b) Solo puede haber un certificado, que es el que el servidor envía al cliente
c) El servidor podría requerir también un certificado del usuario, aunque no es común
d) No hay certificados con claves públicas, ya que se usa criptografía asimétrica

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