Nombre y apellidos:
Grupo:
Fecha:

Instrucciones generales para las preguntas cerradas:

- Marca solamente la respuesta más apropiada en cada caso, en la tabla de respuestas
- 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 solamente las preguntas en las que estés seguro. Una respuesta incorrecta resta un tercio del valor de una respuesta acertada. Una pregunta sin responder no resta puntos.

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

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		33		34		35	
36		37		38		39		40	
41		42		43		44		45	
46		47		48		49			

1. Una persona que extrae y analiza los datos que se transmiten por una línea de comunicación es un

   a) Sniffer
   b) Phreaker
   c) Hacker
   d) DoS

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) Spoofing
   c) Sniffer
   d) Keylogger

3. El phishing

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

4. 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

5. Un adware

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

6. Es spyware

   a) Todos los virus
   b) Todos los spoofing
   c) Todos los keyloggers
   d) Todos los adware

7. Si comparamos un ataque DOS con un DDOS

   a) Un ataque DDOS es más fácil de evitar
   b) Un ataque DDOS suele estar originado en una botnet
   c) Un ataque DOS suele tener mayor impacto que uno DDOS
   d) Un ataque DOS es un tipo de ataque DDOS

8. Un malware que modifica otros ficheros ejecutables para que contengan copias del malware es un

   a) Virus
   b) Troyano
   c) Adware
   d) Hoax

9. Un malware que se propaga, pero sin modificar otros ficheros ejecutables, es un

   a) Gusano
   b) Troyano
   c) Hoax
   d) Virus

10. 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

11. La llamada a casa de un malware

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

12. Un troyano se caracteriza porque

    a) Roba contraseñas, especialmente de cuentas de banco

b) El usuario colabora en su instalación en el sistema

c) Instala un keylogger

d) Se instala a través de spam

13. La clasificación de los malwares (virus, ransomware, addware, gusano,...) se suele basar en

a) Por su nivel de impacto en la seguridad

b) Por la forma en que se combate desde las políticas de seguridad

c) Por el tipo de hacker que lo ha creado

d) Por su forma de propagación y las acciones de su payload

14. La ingeniería social

a) Se basa en el comportamiento social usual de las personas

b) Consiste en manipular sistemas biométricos de autentificación

c) Se utiliza para hacer sniffing

d) Encuentra formas de construir contraseñas que las personas puedan recordar fácilmente

15. Un mensaje en el que se da una noticia impactante, pero de baja credibilidad, es un

a) Phishing

b) Hoax

c) Troyano

d) Spam

16. Generalmente, se utiliza el email para enviar spam porque

a) Es el método tradicional

b) Es más fácil engañar a un antivirus con un email que, por ejemplo, con Whatsapp

c) No es fácil conseguir otro tipo de direcciones de personas, por ejemplo, de Whatsapp

d) Permite llegar a más gente, con menor inversión en dinero y tiempo

17. Las actualizaciones de software

a) No son importantes para la seguridad, excepto la del antivirus

b) Deben retrasarse lo más posible, porque son una fuente de troyanos (excepto la actualización del antivirus)

c) Son importantes para la seguridad, ya que pueden arreglar vulnerabilidades

d) No son importantes para la seguridad, pero sí para el usuario, ya que añaden nuevas funcionalidades

18. Las actividades del _____ se orientan a perjudicar al atacado, y a veces a obtener algún provecho de ello

a) Cracker

b) Nerd

c) Samurai

d) Hacker

19. Se llama poisoning, en ocasiones, al

a) Fuerza bruta

b) Spoofing

c) Sniffing

d) Phishing

20. La técnica de la inundación (flooding) suele utilizarse para realizar un ataque de

a) Denial of service

b) DNS spoofing

c) DNS hijacking

d) Sniffing

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

a) Spoofing

b) Phishing

c) Denial of service

d) Fuerza bruta

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

a) Flooding

b) Code injection

c) Denial of service

d) Fuerza bruta

23. El malware más complicado de detectar es

a) Un DOS

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

24. Un exploit es

a) Una vulnerabilidad aun desconocida por el fabricante
b) Una vulnerabilidad ya conocida por el fabricante
c) Un hacker de reconocido prestigio
d) Un software que automatiza los ataques

25. Un rootkit

a) Es un exploit para conseguir privilegios de administrador
b) Modifica el sistema operativo para ocultar la presencia del malware
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

26. Una botnet

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

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

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

28. Los ataques de code injection se caracterizan por

a) Propagarse como un troyano
b) Propagarse como un gusano
c) Aprovechar vulnerabilidades de los programas o servicios para que ejecuten un código elegido por el atacante
d) Provocar una denegación de servicio (DOS)

29. El antivirus puede ejecutarse

a) A demanda
b) Al vuelo y 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

30. Realizar sniffing es más fácil

a) En una red con un switch
b) En una red con un hub
c) El sniffing no puede realizarse en redes ethernet, sólo en redes inalámbricas
d) Es igual de complicado en una red con un hub o un switch

31. Un ataque de flooding es un tipo concreto de

a) Phishing
b) Troyano
c) Man in the middle
d) DOS

32. En una comunicación HTTPS

a) No hay certificados con claves públicas, ya que se usa criptografía asimétrica
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 híbrida
d) El servidor podría requerir también un certificado del usuario, aunque no es común

33. 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

34. La autenticación consiste en

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

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

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

36. ¿Para qué puede utilizar un "hidden volume" de TrueCrypt?

a) Para poder presentar un conjunto de ficheros creible, pero falso
b) Todos los discos son "hidden", porque los datos están encriptados
c) El concepto de "hidden volume" no es de TrueCrypt, se aplica a los discos no montados en el fichero /etc/fstab
d) El concepto de "hidden volume" no es de TrueCrypt, se aplica a los discos externos en la BIOS para no arrancar desde ellos

37. 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 encriptar los ficheros
c) Hay que firmar y encriptar los ficheros
d) Basta con firmar los ficheros

38. La criptografía híbrida

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

39. En un sistema de clave simétrica

a) No es posible desencriptar sin la clave privada
b) Es un problema el intercambio de claves, ya que si un tercero intercepta la clave puede cambiar las firmas electrónicas
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

40. En un sistema de clave asimétrica

a) Se encripta solamente con la clave privada, y se desencripta solamente con la clave pública
b) Se encripta solamente con la clave pública, y se desencripta solamente con la clave privada
c) Se encripta con una de las claves (privada o pública), y se desencripta con la otra clave
d) Se encripta con una de las claves (privada o pública), y se desencripta con la misma clave

41. Para conseguir una firma electrónica se necesita

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

42. Son funciones resumen

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

43. 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 el intercambio de claves

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

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

---

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

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

b) Es más difícil y caro realizar programas que lo implementen

c) Es menos seguro el intercambio de claves

d) Es más lento, por el tiempo de proceso

---

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

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

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

c) Aumentar la confidencialidad

d) Aumentar el objetivo de "no repudio"

---

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

a) 2 claves (dos públicas)

b) 3 claves (dos públicas y una privada)

c) 3 claves (una pública, una privada y una simétrica)

d) 2 claves (una pública y una privada)

---

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

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

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 un par de claves (pública y privada)

---

48. Las siglas PKI hacen referencia a

a) El programa que se suele utilizar para la criptografía de clave pública

b) El conjunto de una clave pública y privada, empaquetadas en un certificado x509

c) El conjunto de certificados raíz de mi navegador web

d) El estándar que permite intercambiar claves públicas, y confiar en ellas

---

49. El "Cifrado del César" es

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

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

c) Criptografía estadística, porque se necesitan probar varias posibilidades

d) Criptografía híbrida, porque mezcla métodos manuales y automáticos

50. Describe los posibles pasos a seguir para conseguir una botnet

51. Describe qué medidas pueden tomarse ante el phishing

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

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

a)