

**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	

---

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

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

---

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) Sniffer
- c) Keylogger
- d) Phreaker

---

3. El phishing

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

---

4. Cuando un servicio informático (por ejemplo, una web) es imitado por otro para hacerse pasar por el servicio original, se esta utilizando

- a) Dos
- b) Spamming
- c) Spoofing
- 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 spoofing
- b) Todos los adware

- c) Todos los virus
- d) Todos los keyloggers

---

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

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

---

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

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

---

9. El payload

- a) Es la función maliciosa de un malware
- b) Es el sistema de propagación de un malware
- c) Es un sinónimo de adware
- d) Es un sinónimo de spyware

---

10. La llamada a casa de un malware

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

---

11. Un troyano se caracteriza porque

- a) Roba contraseñas, especialmente de cuentas de banco
- b) Instala un keylogger
- c) El usuario colabora en su instalación en el sistema
- d) Se instala a través de spam

---

12. La ingeniería social

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

- 
- b) Consiste en manipular sistemas biométricos de autenticación
- c) Se utiliza para hacer sniffing
- d) Se basa en el comportamiento social usual de las personas
- 
13. Un mensaje en el que se da una noticia impactante, pero de baja credibilidad, es un
- a) Hoax
- b) Troyano
- c) Spam
- d) Phishing
- 
14. Generalmente, se utiliza el email para enviar spam porque
- a) Es más fácil engañar a un antivirus con un email que, por ejemplo, con Whatsapp
- b) Permite llegar a más gente, con menor inversión en dinero y tiempo
- c) Es el método tradicional
- d) No es fácil conseguir otro tipo de direcciones de personas, por ejemplo, de Whatsapp
- 
15. Las actualizaciones de software
- a) Son importantes para la seguridad, ya que pueden arreglar vulnerabilidades
- b) No son importantes para la seguridad, excepto la del antivirus
- 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)
- 
16. Las actividades del \_\_\_\_\_ se orientan a perjudicar al atacado, y a veces a obtener algún provecho de ello
- a) Nerd
- b) Hacker
- c) Cracker
- d) Samurai
- 
17. Se llama poisoning, en ocasiones, al
- a) Fuerza bruta
- b) Phishing
- c) Sniffing
- d) Spoofing
- 
18. La técnica de la inundación (flooding) suele utilizarse para realizar un ataque de
- a) DNS spoofing
- b) Denial of service
- c) Sniffing
- d) DNS hijacking
- 
19. Para conseguir un ataque man-in-the-middle, suele ser necesario utilizar previamente
- a) Denial of service
- b) Fuerza bruta
- c) Spoofing
- d) Phishing
- 
20. Desde el punto de vista del atacante, un ataque de diccionario es una alternativa a
- a) Fuerza bruta
- b) Flooding
- c) Code injection
- d) Denial of service
- 
21. El malware más complicado de detectar es
- a) Un gusano
- b) Un DOS
- c) Un spam
- d) Un rootkit
- 
22. Un exploit es
- a) Una vulnerabilidad aun desconocida
- b) Un software que automatiza los ataques
- c) Un hacker de reconocido prestigio
- d) Una vulnerabilidad ya conocida
- 
23. Un 0-day (zero day) es
- a) Un software que automatiza los ataques
- b) Una vulnerabilidad ya conocida
- c) Un hacker de reconocido prestigio
- d) Una vulnerabilidad aun desconocida

---

24. Un rootkit

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

---

25. Una bootnet

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

---

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

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

---

27. 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 gusano
- c) Propagarse como un troyano
- d) Provocar una denegación de servicio (DOS)

---

28. El antivirus puede ejecutarse

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

---

29. Realizar sniffing es más fácil

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

---

30. Un ataque de flooding es un tipo concreto de

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

---

31. Explica como un keygen puede utilizarse para distribuir malware

---

32. Describe una buena política de contraseñas, de forma que no puedan hackearse fácilmente aunque se consigan los hashes (resúmenes) de las mismas

---

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

---

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

a)