

# Examen para HE01 - 9,00

## Pregunta 1

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

Los sistemas de tipo Keylogger extraen información almacenada en la memoria RAM de un sistema operativo Microsoft Windows. ¿Verdadero o Falso?:

Seleccione una:

- ☐ Verdadero
- ☒ Falso

Siguiente página

## Pregunta 2

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

¿Cuál de las siguientes herramientas se utilizan en un Reconocimiento pasivo?:

- ☐ a. dig.
- ☐ b. snmpwalk.
- ☐ c. nmap.
- ☒ d. shodan.

[Quitar mi elección](#)

Página anterior

Siguiente página

## Pregunta 3

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

Durante la presentación de resultados únicamente se presentan los resultados de la auditoría, pero no se resuelven dudas ni se dan recomendaciones para solventar las vulnerabilidades. ¿Verdadero o Falso?:

Seleccione una:

- ☐ Verdadero
- ☒ Falso

Página anterior

Siguiente página

## Pregunta 4

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

¿Qué tipo de información podemos recopilar en las redes sociales?:

- ☒ a. Averiguar tecnologías utilizadas en la compañía.
- ☐ b. Direccionamiento IP y servicios expuestos en el perímetro de la empresa.
- ☐ c. Averiguar credenciales de usuarios.
- ☐ d. Activos pertenecientes a las empresas.

[Quitar mi elección](#)

Página anterior

Siguiente página

Pregunta 5

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

Indica cuál de las siguientes herramientas no es un proxy de interceptación:

- ☐ a. Echo Mirage.
- ☐ b. ZAP.
- ☐ c. Burp.
- ☒ d. Shellter.

[Quitar mi elección](#)

[Página anterior](#)

[Siguiendo página](#)

Pregunta 6

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

¿Qué es una vulnerabilidad de tipo 0-Day?:

- ☒ a. Una vulnerabilidad que no es pública.
- ☐ b. Una vulnerabilidad que no existe.
- ☐ c. Una vulnerabilidad que no tiene ningún tipo de impacto ni riesgo.
- ☐ d. Una vulnerabilidad pública.

[Quitar mi elección](#)

[Página anterior](#)

[Siguiendo página](#)

Pregunta 7

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

En que portal podemos buscar exploits específicos para una versión de software en concreto:

- ☐ a. LinkedIn.
- ☐ b. Shodan.
- ☐ c. Censys.
- ☒ d. Exploit-db.

[Quitar mi elección](#)

[Página anterior](#)

[Siguiendo página](#)

Pregunta 8

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

¿Que es la DarkWeb?:

- ☐ a. Contenido que se encuentra disponible de manera pública en internet.
- ☐ b. Contenido utilizado por los ciberdelincuentes pero que se encuentra disponible de manera pública en internet.
- ☒ c. Redes privadas utilizadas por los ciberdelincuentes para ofrecer sus servicios, vender información previamente robada, vulnerabilidades no reportadas a los fabricantes.
- ☐ d. Todo el contenido privado que no se encuentra a disposición del público en general.

[Quitar mi elección](#)

[Página anterior](#)

[Siguiendo página](#)

Pregunta **9**

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Desmarcar

Indica cual de las siguientes opciones es una afirmación correcta para la Fase de Explotación:

- ☐ a. Se detectan vulnerabilidades que puedan existir en los sistemas y servicios
- ☒ b. Se utilizan técnicas para poder aumentar el nivel de privilegios en este sistema.
- ☐ c. Se recopila información acerca de los activos a auditar.
- ☐ d. El objetivo es lograr un primer acceso o de privilegios en los activos.

[Quitar mi elección](#)

Página anterior

Siguiente página

Pregunta **10**

Respuesta guardada

Se puntúa como 0 sobre 1,00

🚩 Marcar pregunta

Para poder inspeccionar los datos transmitidos y recibidos por una interfaz de red, a bajo nivel, que herramienta de las siguientes hay que utilizar:

- ☐ a. arpscan.
- ☐ b. netdiscover.
- ☒ c. wireshark.
- ☐ d. nmap.

[Quitar mi elección](#)

Página anterior

Terminar intento...