ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Laboratorio de ciberseguridad

ESCAPE: Preparing healthcare professionals for cyberattacks	
Laboratorio de ciberseguridad	
Idioma	*Español*

Índice

1. Laboratorio de ciberseguridad..... 3
2. Clasificación..... 3
3. Descripción.....4
4. Más información.....5

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Laboratorio de ciberseguridad	
Idioma	*Español*

1. Laboratorio de ciberseguridad

Un entorno de laboratorio práctico y gamificado donde los participantes pueden practicar hacking ético, seguridad de redes y criptografía mediante simulaciones seguras.

2. Clasificación

Categoría	**Marcar si aplica:**
Sector	☐ Sanitario
	☑ Público general
	☐ Otro
Temas cubiertos	☑ Ciberseguridad
	☐ Protección de datos
Tipo de situación	☑ Prevención
	☐ Impacto (ej. Cuando está ocurriendo o ha ocurrido) en el cuidado del paciente
	☑ Impacto en otras actividades que no implican el cuidado del paciente
Idioma del material original	☐ Neerlandés
	☑ Inglés
	☐ Alemán
	☐ Italiano

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Laboratorio de ciberseguridad	
Idioma	*Español*

	☐ Español
Tipo del material	☑ Preguntas de cuestionario.
	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3. Descripción

1. ¿Qué es el hacking ético?

   a) Robar datos por diversión

   b) Hacking autorizado para probar la seguridad

   c) Propagar malware de forma legal

   d) Trucos de juegos

   Respuesta correctar: Hacking autorizado para probar la seguridad
   Feedback: Los hackers éticos ayudan a **fortalecer los sistemas** identificando vulnerabilidades antes de que los atacantes puedan explotarlas.

2. ¿Qué es un entorno sandbox?

   a) Un lugar para probar amenazas de manera segura

   b) Amplificador de Wi-Fi

   c) Unidad de copia de seguridad

   d) Generador de contraseñas

   Respuesta correcta: Un lugar para probar amenazas de manera segura
   Feedback: Los *sandboxes* aíslan los riesgos y permiten probar software o amenazas sin afectar los sistemas reales.

3. ¿Qué protege la criptografía?

   a) La velocidad del hardware

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

b) La confidencialidad de los datos

c) El diseño de aplicaciones

d) El uso de batería

Respuesta correcta: La confidencialidad de los datos
Feedback: El cifrado garantiza que solo los usuarios autorizados puedan **leer la información sensible**.

4. What is a brute-force attack?

a) Intentar todas las combinaciones posibles de contraseñas

b) Instalar ransomware

c) Bloquear sitios web

d) Enviar correos de phishing

Respuesta correcta: Intentar todas las combinaciones posibles de contraseñas
Feedback: Los ataques de fuerza bruta son lentos pero **peligrosos si no existen protecciones** como bloqueo de intentos o autenticación multifactor.

5. ¿Qué es una prueba de penetración (*penetration testing*)?

a) Crear contraseñas fuertes

b) Simulaciones de ciberataques para encontrar debilidades

c) Limpiar virus

d) Bloquear anuncios

Respuesta correcta: Simulaciones de ciberataques para encontrar debilidades
Feedback: Las pruebas de penetración permiten **identificar vulnerabilidades de manera temprana** y fortalecer la seguridad de los sistemas.

4. Más información

- Fuente: LabEx Free Cybersecurity Labs

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.