



# Reporte Generador de Escenarios de Aprendizaje

Nombre de Usuario:

aa

Consulta:

sss

Respuesta de la IA:

¡Hola! Soy un experto en hackatones. Estoy aquí para ayudarte con cualquier pregunta sobre malware, programación y ciberseguridad.

Por favor, indícame tu nombre: \_\_\_\_ y tu nota: \_\_\_\_.

### Información básica del ciberataque

Ciberataque: Troyano

Los troyanos son un tipo de malware que se presenta como un software legítimo para engañar a los usuarios y hacer que lo instalen. Una vez dentro del sistema, pueden robar información, crear puertas traseras o realizar otras acciones maliciosas.

### Ejemplo de cómo te pueden infectar

Un usuario puede infectarse al descargar un archivo adjunto de un correo electrónico que parece ser de una fuente confiable, pero en realidad contiene un troyano.

### Código de ejemplo de funcionamiento

```
python
```

```
import os
```

```
def troyano():
```

```
    # Simula la creación de un archivo en el sistema
```

```
    with open("archivo_infectado.txt", "w") as f:
```

```
        f.write("Este archivo es inofensivo, pero contiene un troyano.")
```

```
    os.system("notepad archivo_infectado.txt") # Abre el archivo en el bloc de notas
```

```
troyano()
```

### Actividad solicitada

Preguntas tipo test sobre troyanos:

1. ¿Qué es un troyano?

- a) Un tipo de virus
- b) Un software legítimo que oculta malware
- c) Un programa antivirus

2. ¿Cómo se propagan comúnmente los troyanos?

- a) A través de redes sociales

- b) Mediante correos electrónicos con archivos adjuntos maliciosos
- c) A través de actualizaciones de software

3. ¿Cuál es una de las consecuencias de un troyano en un sistema?

- a) Mejora el rendimiento del sistema
- b) Roba información personal
- c) Aumenta la seguridad del sistema

### Respuestas de la actividad

- 1. b) Un software legítimo que oculta malware
- 2. b) Mediante correos electrónicos con archivos adjuntos maliciosos
- 3. b) Roba información personal

Espero que esta actividad te sea útil. Si tienes más preguntas, no dudes en preguntar.



**Reporte del Usuario:**

dsisisiisii