

## Práctica de laboratorio: Visualizar a los Hackers de Sombrero Negro

### Objetivos

Investigar y analizar incidentes de ciberseguridad

### Aspectos básicos/Situación

El FBI ha estimado que el cibercrimen costó a individuos y empresas más de 3.5 billones de dólares en 2019. Los gobiernos, las empresas y los usuarios individuales cada vez son víctimas de más ciberataques, y los incidentes de ciberseguridad se están volviendo más habituales.

En esta práctica de laboratorio, crearán tres ciberatacantes hipotéticos, cada uno con una organización, un ataque y un método para que una organización impida o mitigue el ataque. Además, sugiera un método mediante el cual una organización podría prevenir o mitigar el ataque.

**Nota:** Puede utilizar el navegador web de la máquina virtual instalada en una práctica de laboratorio anterior para investigar problemas de seguridad. Si utilizan la máquina virtual, pueden impedir que se instale malware en su computadora.

### Recursos necesarios

- PC o dispositivo móvil con acceso a Internet y máquina virtual (opcional)

## Instrucciones

### Situación 1:

- a. ¿Quién es el atacante?
  
  
  
  
  
  
- b. ¿A qué organización o grupo está asociado el atacante, si lo hay?
  
  
  
  
  
  
- c. ¿Cuál es el motivo del atacante?
  
  
  
  
  
  
- d. ¿Qué método de ataque se utilizó?
  
  
  
  
  
  
- e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?
  
  
  
  
  
  
- f. ¿Cómo se podría prevenir o mitigar este ataque?

**Situación 2:**

- a. ¿Quién es el atacante?
  
  
  
  
  
  
- b. ¿Con qué organización y/o grupo está asociado el atacante?
  
  
  
  
  
  
- c. ¿Cuál es el motivo del atacante?
  
  
  
  
  
  
- d. ¿Qué método de ataque se utilizó?
  
  
  
  
  
  
- e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?
  
  
  
  
  
  
- f. ¿Cómo se podría prevenir o mitigar este ataque?

**Situación 3:**

- a. ¿Quién es el atacante?
  
  
  
  
  
  
- b. ¿Con qué organización y/o grupo está asociado el atacante?
  
  
  
  
  
  
- c. ¿Cuál es el motivo del atacante?
  
  
  
  
  
  
- d. ¿Qué método de ataque se utilizó?
  
  
  
  
  
  
- e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?
  
  
  
  
  
  
- f. ¿Cómo se podría prevenir o mitigar este ataque?