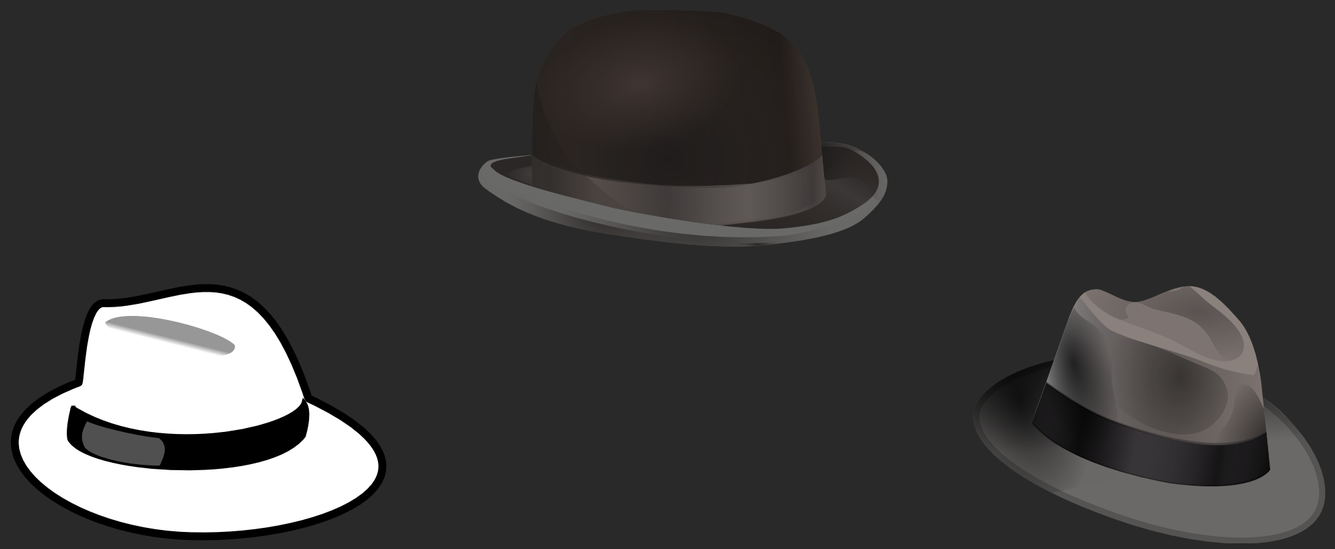
HACKING ÉTICO

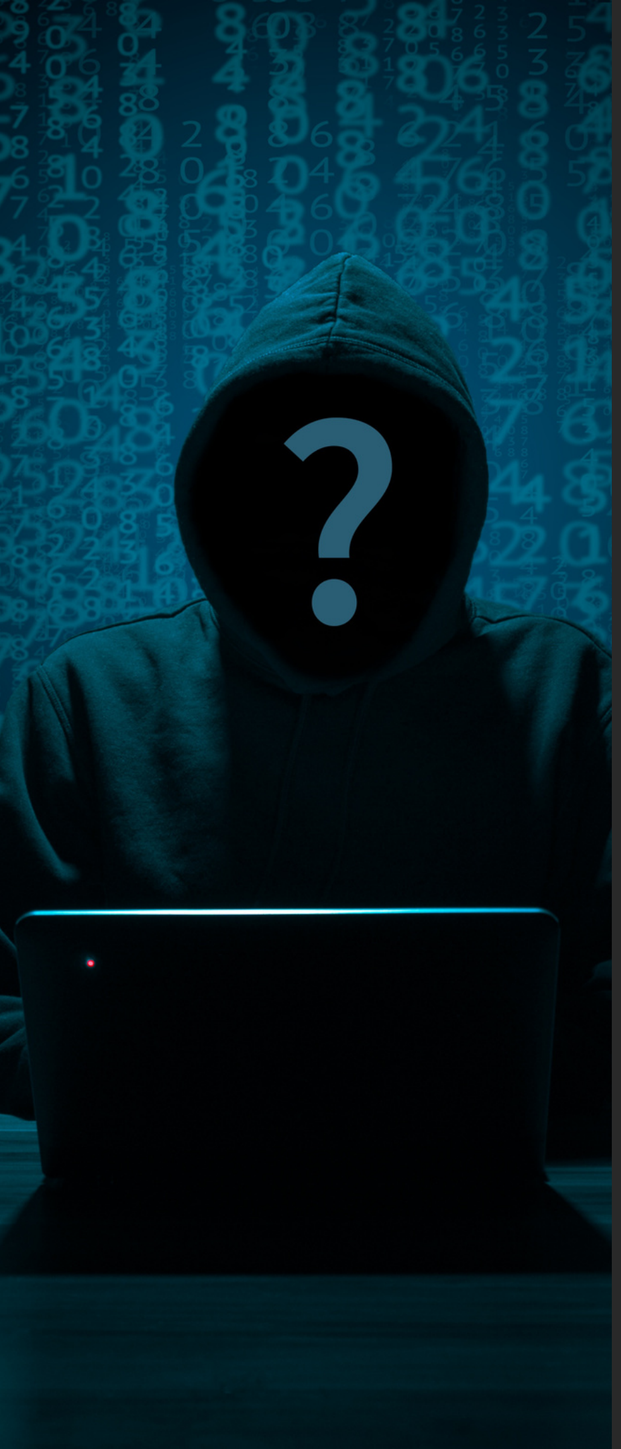
"White hat hacker"

3CV11

RAMIREZ BENITEZ BRAYAN

El hacking ético en ciberseguridad se ha convertido en una de las herramientas más importantes para mejorar la seguridad de los sistemas, reduciendo sus vulnerabilidades y aplicando las medidas necesarias para evitar o minimizar los ataques externos.





¿Qué es el hacking ético?

Hace referencia al modo en que una persona, utiliza todos sus conocimientos sobre informática y ciberseguridad para hallar vulnerabilidades o fallas de seguridad dentro de un sistema.

Los hackers de sombrero blanco, son expertos en seguridad de la información que irrumpen en los sistemas informáticos por petición de sus clientes.

¿En que consiste el hacking ético?

Consiste en atacar de una forma pasiva el entorno de seguridad que ha creado la empresa que solicita este tipo de servicio.

En caso de encontrar algún error o alguna vulnerabilidad mediante un informe completo se obtienen soluciones para mejorar la ciberseguridad de la organización en cuestión.

¿Qué es un test de penetración en hacking ético?

Es una metodología que consiste en planificar un ataque a una red o plataforma, sin importar su tamaño, para encontrar vulnerabilidades en ella. Para conseguirlo, es necesario simular diferentes patrones de ataque empleando herramientas desarrolladas por métodos de ataque conocidos.

Algunos de los componentes de un test de penetración

- ***Puertos de seguridad***
- ***Elementos de acoplamiento***
- ***Servidores***
- ***Equipos de telecomunicaciones***
- ***Aplicaciones web***
- ***Instalaciones de infraestructura***
- ***Conexiones inalámbricas***

Generalmente, los test de penetración se clasifican en:

PRUEBAS DE CAJA NEGRA

Donde los especialistas en hacking ético solo tienen a su disposición la dirección de la red.

PRUEBAS DE CAJA BLANCA

Donde el punto de partida es un amplio conocimiento de los sistemas.

Principales beneficios

1. Ahorrar dinero en la implementación de sistemas de seguridad eficientes
2. Impedir catástrofes públicas por ser víctima de algún ataque hacker fuerte
3. Organizar y mantener los sistemas de ciberseguridad para evitar filtraciones
4. Focalizar las inversiones en seguridad eficientemente y no malgastar en sistemas con fallas
5. Concientizar a todos los colaboradores sobre la importancia que supone poner en riesgo los sistemas por el mal uso de contraseñas poco seguras

Hacking ético vs. hackeo

El ético tiene como fin principal brindar protección a las infraestructuras digitales y los datos confidenciales de los ataques para mejorar la seguridad.

El hackeo, se centra especialmente en objetivos malintencionados y destructivos como infiltración y destrucción de sistemas de seguridad.

Gracias por su atención!