
DAKAR IT
netcheck
services
Un servicio de Dakar IT

¿QUÉ ES NETCHECK SERVICES?

Dakar IT entiende la importancia de los activos informaticos dentro de las organizaciones, ya que la explotación de vulnerabilidades es uno de los mayores temores que afrontan las empresas.

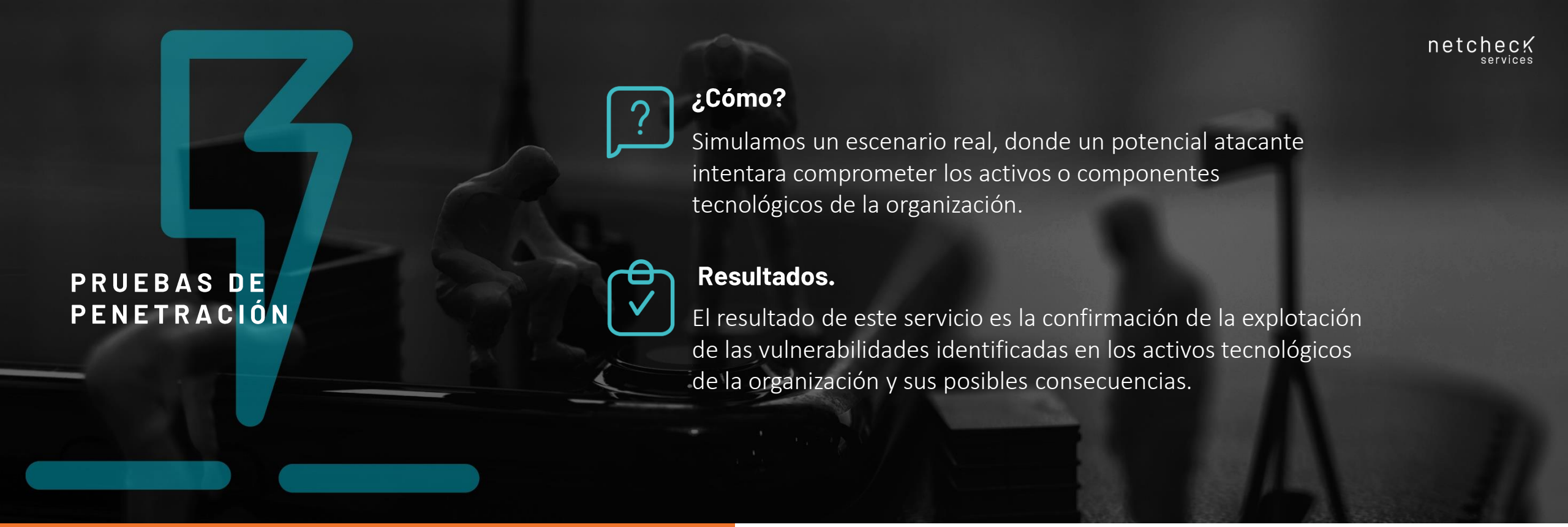
Por ello es importante, enfocar los esfuerzos en identificar los puntos débiles, antes que terceros o usuarios mal intencionados aprovechen estas debilidades y poner en riego la operación y credibilidad del negocio.

Por esta razón, como medida preventiva te presentamos nuestros **Servicios de Ciberseguridad** y realizar una evaluación de las brechas de seguridad, que permita identificar el nivel de criticidad y los posibles impactos asociados.

- **Pruebas de penetración**
- **Análisis de malware**
- **Análisis de vulnerabilidades**
- **Análisis de código**

Trabajamos con expertos en ciberseguridad, respaldando su conocimiento con certificaciones como:

CHE,CISSP, CSX, CDPS.



PRUEBAS DE PENETRACIÓN

netcheck services

¿Cómo?

Simulamos un escenario real, donde un potencial atacante intentara comprometer los activos o componentes tecnológicos de la organización.

Resultados.

El resultado de este servicio es la confirmación de la explotación de las vulnerabilidades identificadas en los activos tecnológicos de la organización y sus posibles consecuencias.

Propuesta de valor:

- ✓ Generar información relevante para la organización sobre la postura de seguridad existente en sus componentes tecnológicos.
- ✓ Recomendaciones de las actividades requeridas para mitigar las vulnerabilidades en los activos tecnológicos.

Las técnicas utilizadas para las pruebas de penetración pueden ser:

Caja negra: El cliente comparte el mínimo de información, posteriormente se realiza una recopilación de información desde fuentes abiertas de este primer alcance definido.
Después de recopilar la suficiente información, se comparten los hallazgos al cliente con la finalidad de que el cliente defina concretamente cuál sería el alcance final para el servicio. (Esto ayuda al cliente a conocer la información que su organización expone a internet).

Caja gris: El cliente proporciona el alcance final, los activos que desea sean evaluados en este tipo de servicio desde un origen externo o interno.

DAKAR IT

METODOLOGÍA PARA LAS PRUEBAS DE PENETRACIÓN

La ejecución de las pruebas de seguridad se realizan con metodologías estándar como: **OSSTMM, OWASP y SANS**.
La **metodología utilizada por Dakar IT** se compone de las siguientes fases:

1. Reconocimiento: Esta etapa consiste en recolectar la información pública disponible sobre un objetivo y que pudiera ser utilizada para desarrollar de una mejor manera las siguientes etapas de las pruebas de penetración.

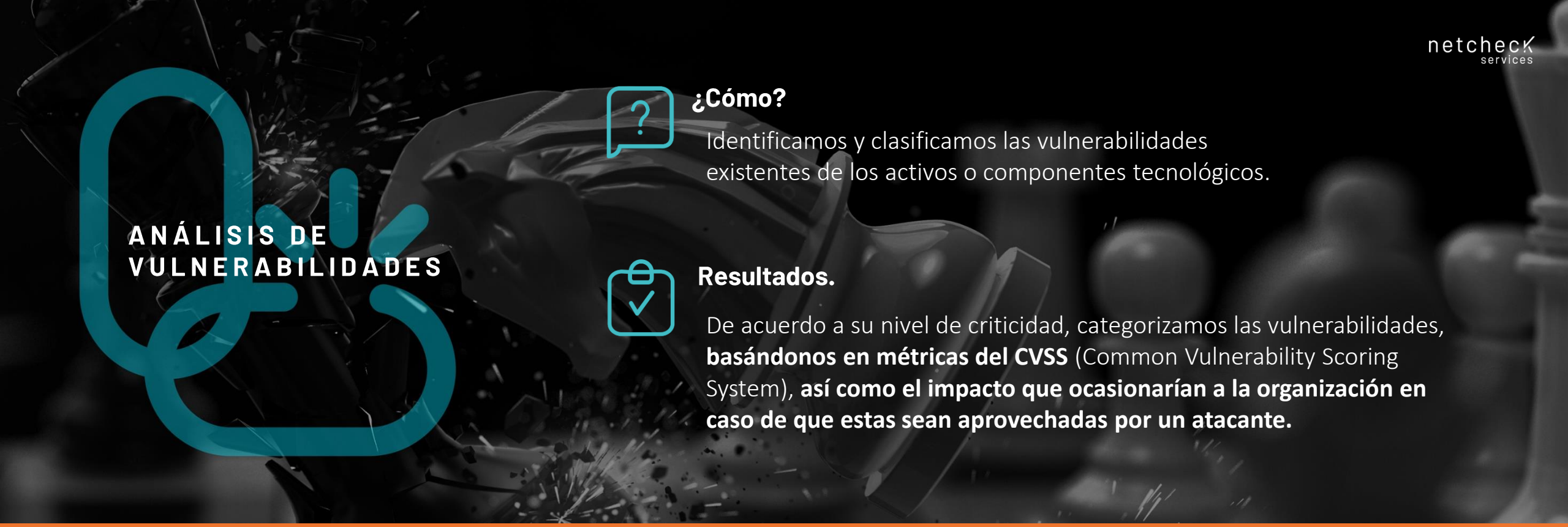
2. Enumeración: Consiste en interactuar directamente con la infraestructura o componentes del cliente con la finalidad de identificar ciertas características y obtener mayor información del objetivo.

3. Análisis de vulnerabilidades: Se realiza la identificación de vulnerabilidades en los activos definidos como parte del alcance.

4. Explotación: Se realiza el intento de explotación de las vulnerabilidades identificadas previamente con la finalidad de obtener control o demostrar otras técnicas de compromiso que un atacante real podría ejecutar.

5. Post Explotación: Una vez que se ha explotado una vulnerabilidad se pueden realizar actividades adicionales dependiendo del alcance, que en este caso pueden ser algunas de las siguientes: pivoteo entre sistemas, movimientos laterales o escalación de privilegios.

6. Resultados: Se generan reportes que demuestren de forma clara los resultados obtenidos.
Se generan planes de acción sugeridos para mitigar las vulnerabilidades.



netcheck
services

ANÁLISIS DE VULNERABILIDADES

¿Cómo?

Identificamos y clasificamos las vulnerabilidades existentes de los activos o componentes tecnológicos.

Resultados.

De acuerdo a su nivel de criticidad, categorizamos las vulnerabilidades, **basándonos en métricas del CVSS** (Common Vulnerability Scoring System), **así como el impacto que ocasionarían a la organización en caso de que estas sean aprovechadas por un atacante.**

Propuesta de valor:

- ✓ Documentar la postura de riesgo asociada a la vulnerabilidad y el impacto asociado.
- ✓ Realizamos una categorización de acuerdo a su nivel de criticidad y su impacto.
- ✓ Recomendaciones o sugerencias de las actividades requeridas para mitigar las vulnerabilidades.
- ✓ Se recomienda validar después de un periodo si los planes de remediación han sido ejecutados correctamente realizando nuevamente otro análisis de vulnerabilidades sobre el mismo alcance.

DAKAR IT

ANÁLISIS DE MALWARE

¿Cómo?

El análisis permite identificar el comportamiento que ejecuta una muestra de malware que esté afectando a la organización.

Resultados.

- Entender su manera de propagación.
- Intentar identificar los TTPs (**T**actics, **T**echniques and **P**rocedures) del atacante.
- Reconocer si este malware pertenece a un ataque dirigido a la organización - **Advanced Persistent Threat** (APT).
- Identificar los **IOC** (Indicator of Compromise) que ayudan a una organización a protegerse al introducir estos IOC en sus equipos de seguridad perimetral; los IOC pueden ser: Direcciones IP, valores Hash, dominios o URLs.

Propuesta de valor:

- ✓ Generar información relevante para que la organización afectada por un malware se proteja en caso de ya haber sido comprometidos o de posibles nuevas propagaciones del mismo.
- ✓ Recomendaciones de las actividades requeridas para protegerse ante amenazas de malware

ANÁLISIS DE CÓDIGO

¿Cómo?

Análisis Estático: Contempla el análisis basado en megas de código (fuente u objeto) desarrollado por el cliente en adelante, sin importar el nombre o nombres que pueda tener la aplicación y sin contemplar códigos de terceros, imágenes y datos.

Análisis códigos de terceros: Es muy común la utilización de códigos de terceros u opensource en las aplicaciones, por lo que Veracode pone a su disposición el análisis de estas librerías utilizando un producto adicional denominado Software Composition Analisis, mediante el cual podremos analizar vulnerabilidades en dichos códigos sin importante que sea código fuente objeto, siempre y cuando este soportado por Veracode.

Análisis Dinámico: Contempla el análisis de una dirección URL o IP sin importar el tamaño de la misma. (código en ejecución Internet – Intranet).

Resultados.

Mitigar las vulnerabilidades dentro de los aplicativos de su organización tomando como premisa el código analizado.

Propuesta de valor:

- ✓ Generar información relevante acerca de las vulnerabilidades existentes en el ciclo de vida del desarrollo del software.
- ✓ Entrega de plan de remediación de las vulnerabilidad y vicios del código.

netcheck
services

Un servicio de Dakar IT

Contáctenos directamente en:
ventas@dakarit.com
Tel. (55) **59857868**
www.dakarit.com

DAKAR IT

La **ciberseguridad** es
responsabilidad de todos.