Hacking Ético

SERVICIOS DE CIBERSEGURIDAD

SERVICIOS DE HACKING ÉTICO

INTRODUCCIÓN

La seguridad informática continúa creciendo debido a que **los intentos de vulnerar activos informáticos también siguen al alza**. Las redes y aplicaciones son **vulneradas para ser aprovechadas por terceros** para robar información crítica, cobrar recompensas o simplemente difamar el objetivo, obligando a las empresas a incurrir en costos enormes tanto en su reputación como monetarios **luego de que se concreta un ataque por parte de terceros**.

La forma más efectiva para **conocer las vulnerabilidades y mitigar** los accesos no autorizados es **ejecutar Hacking Ético sobre activos informáticos** que tienen algún nivel de exposición.

Este servicio **simula un ataque informático sobre activos individualizados** estableciendo las vulnerabilidades presentes en las redes, sistemas o aplicaciones definidas. **Durante el ataque se usan herramientas utilizadas por hackers para conocer las vulnerabilidades y explotar las mismas hasta obtener acceso**. El tipo de ataque, junto con la profundidad de éste se acuerdan con anterioridad de tal forma de mitigar o eliminar las vulnerabilidades encontradas.

El servicio evacuará un **reporte** que le permitirá al cliente **conocer las vulnerabilidades y corregir los problemas encontrados.**

¿Por qué IIA?

Confianza

Más de 30 años de experiencia apoyando a las empresas chilenas, entregando **confiabilidad** y **privacidad** a cada uno de nuestros clientes en el mercado de las Tecnologías de la Información. Desde armado de equipos, informática, Ingeniería e Internet hasta servicios de Datacenter y Seguridad de la Información, logrando así un proceso que cuenta con el respaldo de una empresa experimentada.

Más de 3.000 empresas avalan nuestra trayectoria y dedicado compromiso en lo que hacemos.

Experiencia

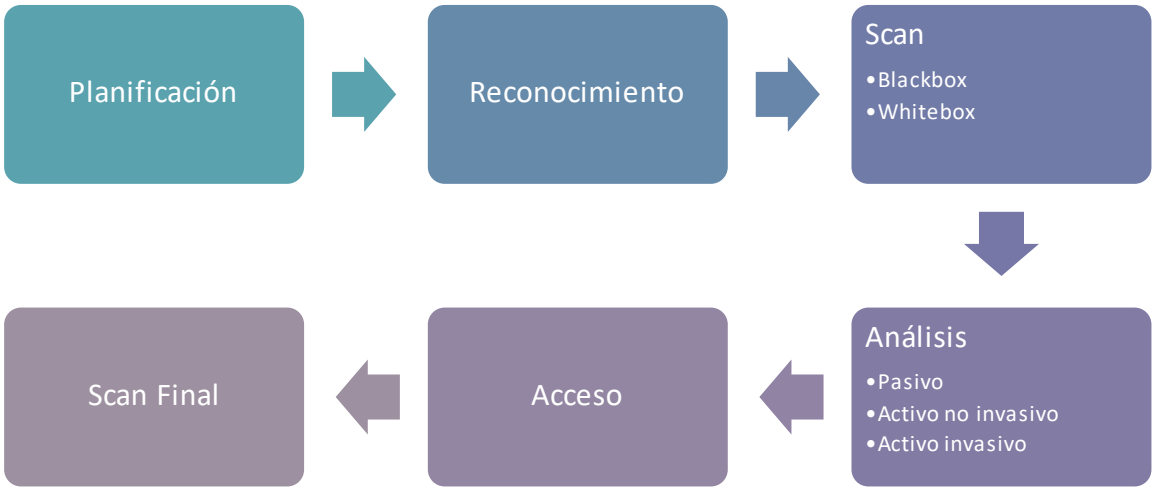
IIA posee **certificación ISO27001** vigente por más de 5 años consecutivos, lo que asegura al cliente experiencia necesaria **aplicando sistemas de gestión, buenas prácticas de seguridad informática**, así como la mejora continua de sus procesos y en el manejo de información crítica para nuestros clientes.

Know-How

IIA cuenta con **personal capacitado y herramientas líderes** usadas en el rubro para escanear las últimas vulnerabilidades conocidas y para intentar explotarlas de forma que nuestros clientes puedan aplicar las recomendaciones necesarias para proteger sus redes, sistemas y aplicaciones. Algunas de ellas son Nessus, Metasploit y Kali Linux entre otras.

Proceso

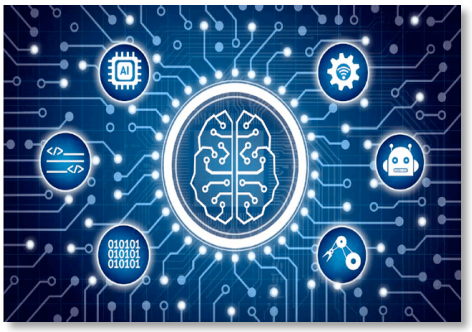
IIA adhiere a procesos conocidos en la Industria de servicios de seguridad que permiten a nuestros clientes obtener lo que necesitan de acuerdo a normas predefinidas que se ajustan a un marco de trabajo que permita analizar los resultados por etapas.



PLANIFICACIÓN

En la etapa de planificación **se acuerdan los plazos y objetivos de la actividad** afinando los detalles del tipo de reconocimiento, scan y acceso que el cliente desea. Como parte de esta etapa se **firma un acuerdo de confidencialidad** que establece las autorizaciones y responsabilidades adecuadas y permitirán el desarrollo de la actividad de forma segura para todas las partes.

RECONOCIMIENTO



La etapa de reconocimiento considera **buscar y obtener información** del objeto destino que está **disponible libremente** y que puede apoyar en el hackeo que se desea realizar. Puede incluir **técnicas de ingeniería social, uso de medios de comunicación establecidos.** En la mayoría de los casos el mismo proceso entrega información para abordar la manera de intentar hackear el objeto.

SCAN

Esta etapa se refiere a **descubrir las vulnerabilidades que pueden estar presentes**. Se realiza usando herramientas manuales y automatizadas. El tipo de scan a ejecutar puede ser de dos tipos:

BLACKBOX

El scan **se realiza sin tener información previa del objetivo**. Sólo se cuenta con las fuentes conocidas públicamente o en herramientas expuestas al público, además de los métodos usados en la etapa de reconocimiento. Se usa cuando el contratante desea **probar las medidas de seguridad existentes** que protegen tanto la arquitectura del objetivo como la información.

WHITEBOX

El contratante provee información formal acerca del objetivo. Normalmente se realiza cuando se desea **evaluar partes específicas de una red o aplicación o simular un intento de vulneración por parte de agentes internos**. Puede ser un nombre de usuario para acceder a una red o aplicación que permita un acceso inicial mayor al que tiene un agente externo a la organización.

ACCESO

Luego de obtener información del objetivo y los servicios o vulnerabilidades disponibles, se intenta **usar las vulnerabilidades encontradas para forzar el acceso a los objetivos descubiertos**. Este acceso puede realizarse siguiendo los siguientes lineamientos: Pasivo, Activo no invasivo, Activo invasivo.

PASIVO

Este intento de acceso es el que requiere menos esfuerzo y tiene como objetivo **establecer si es posible explotar las vulnerabilidades encontradas** sin llegar a concretar un acceso más allá de los objetivos establecidos.

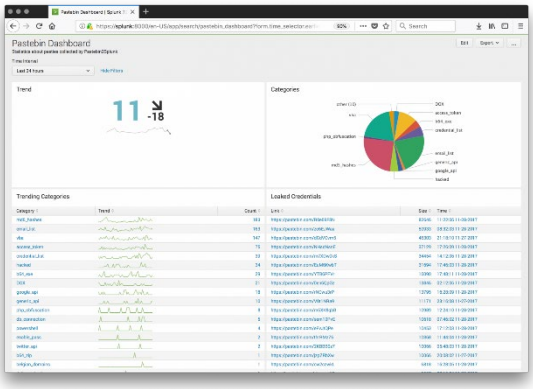
ACTIVO NO INVASIVO

En esta metodología se intenta **explotar las vulnerabilidades presentes** en los sistemas **llegando a ingresar a los objetivos y mantener cierto nivel de acceso** que permita acceder a otros niveles de la infraestructura vulnerada.

ACTIVO INVASIVO

La tercera opción es **explotar las vulnerabilidades** de tal forma de encontrar formas de **obtener información sensible y control de sistemas** que permitan establecer los límites a los que podrían llegar intentos de hackeo maliciosos.

Reporte



La etapa final del proceso se refiere a **documentar los descubrimientos** obtenidos en cada etapa del proceso de tal forma que el cliente pueda usar la información para revisar sus procedimientos y sistemas de seguridad presentes. El **reporte incluye también recomendaciones** de acuerdo a las vulnerabilidades encontradas, de tal forma que el cliente pueda **tomar medidas de mitigación adecuadas** que eviten que las vulnerabilidades sean explotadas.

Scan Final

Luego de que el cliente aplique las recomendaciones y resuelva los problemas expuestos, se realiza un nuevo **escaneo de vulnerabilidades** para determinar si las acciones tuvieron el efecto deseado para evitar posibles ataques. Este escaneo se realiza apuntando específicamente a los problemas encontrados y no buscando nuevas posibilidades de acceso.

Comparativo

Item	Scan		Acceso			Informe	Scan Final
	Reconocimiento		Pasivo	Activo No-Invasivo	Activo Invasivo		
Hacking Ético Pasivo	✓	✓	✓			✓	✓
Hacking Ético Activo No Invasivo	✓	✓		✓		✓	✓
Hacking Ético Activo Invasivo	✓	✓			✓	✓	✓

Para más información contáctenos y solicite un presupuesto formal

CONTACTAR

228401000 – División Internet

30 AÑOS Generando soluciones integrales para su empresa