# Hacking Ético

A2SECURE

## Compruebe la efectividad de sus medidas de seguridad mediante la simulación de ataques reales

El equipo de A2SECURE, mediante su destreza para la simulación de ataques de seguridad, posibilita una perspectiva global para la mejora de la seguridad integral y la eficiencia operativa, la reducción del riesgo y el cumplimiento de normas específicas.

### Pensar de manera Ofensiva para mejorar las Defensas

La explotación de vulnerabilidades existentes se ha convertido en la causa más frecuente de las brechas de seguridad. Es esencial poder verificar que las aplicaciones, redes y sistemas no sean vulnerables a un riesgo de seguridad para evitar que las vulnerabilidades no puedan ser explotadas por usuarios no autorizados o malintencionados. No sería suficiente, sin embargo, un análisis de vulnerabilidades para la identificación de las mismas, sino que además sería fundamental valorar el verdadero impacto que pueden suponer en caso de ser explotadas, y qué medidas efectivas tienen que ser adoptadas al respecto.

### A2SECURE: la solución

A2SECURE combina la singularidad de cada cliente específico con una metodología sistemática que garantiza un servicio integral de calidad. Orquestando nuestras acciones guiadas por los mejores estándares de la industria, con el valor añadido de nuestras tácticas diseñadas in-house, en continuo desarrollo por parte de nuestro equipo de pentesters.

Tenemos claro que una de las claves de nuestro éxito reside en poder trasladar y poner en valor nuestra actividad. El informe final de compilación de resultados, acompañado de una reunión personalizada, facilita la comprensión de los hallazgos y la puesta en marcha de la fase de mitigación siempre con nuestro acompañamiento.

### Hacking Ético: el método

El hacking ético responde a la temida pregunta ¿puede un atacante entrar en mi red? Las pruebas de intrusión identifican las vulnerabilidades que un atacante malintencionado utilizaría para entrar en su organización posibilitando la mitigación de las mismas. Su organización obtiene un entendimiento mayor de su entorno y le permitirá definir una estrategia de fortalecimiento de la seguridad frente a ciberataques potenciales y específicos que aprovechen las vulnerabilidades ya existentes en su organización.

Diseñamos los tests similares a los que podrían emplear los atacantes para mostrar cómo obtendrían acceso no autorizado al entorno de su organización. Desde la búsqueda de información pública a través de OSINT, credenciales de usuarios comprometidas, explotación de vulnerabilidades, pivoting entre redes… hasta alcanzar la persistencia. Sacamos partido de la mínima falla en toda su red para comprometer aquello que verdaderamente debería preocuparle.

### Beneficios

- Determinar el riesgo real de que se vea comprometida la seguridad en su organización
- Disponer de un plan de acción con las medidas y las acciones a realizar para mitigar y reducir el riesgo
- Incrementar la seguridad al poder poner a prueba las medidas defensivas existentes de forma controlada, y evaluar así la efectividad de las mismas y el nivel de respuesta de los equipos de IT
- Satisfacer el cumplimiento de los requisitos normativos y legales tales como HIPAA, PCI-DSS, FFIEC, entre otros
- Remediación de las vulnerabilidades mediante un plan definido y acompañado por los expertos profesionales de A2SECURE

## Diferentes Enfoques y Personalizaciones

Los Pentests de A2SECURE se pueden realizar desde una perspectiva externa, es decir, evaluar las amenazas a nivel perimetral de la red, o bien dentro de la red, a nivel interno.

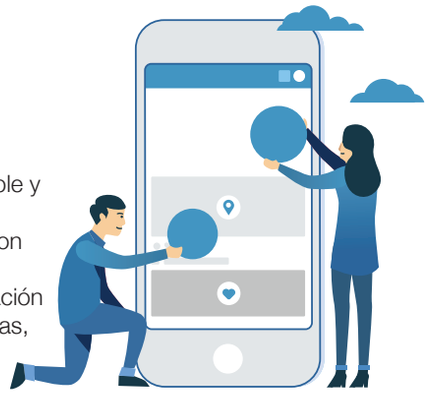
Las auditorías de redes Wi-Fi identifican qué dispositivos inalámbricos están accediendo a su red, determinan los puntos de acceso no autorizados existentes y evalúan la seguridad de la infraestructura Wi-Fi.

Los Test de intrusión de aplicaciones para iOS y Android, así como de dispositivos IoT, identifican posibles brechas de seguridad a nivel de código de aplicación, potenciales fugas o extracciones de datos, y vulnerabilidades que puedan ser explotadas o alteren el funcionamiento de la aplicación

## Qué esperar en su informe

- **Resumen ejecutivo**, dirigido a la audiencia no técnica: gerencia, auditores, junta directiva u otros interesados.
- **Resumen Técnico**, describiendo los problemas identificados y los hallazgos de alto riesgo, y nuestras recomendaciones para remediarlos o reducir el riesgo.
- **Informe Técnico**, dirigido a los empleados técnicos de la organización, proporciona los hallazgos y evidencias encontradas, así como los detalles referentes a:
  - Metodología: detalle de las actividades y las pruebas realizadas siguiendo procedimientos estándares de la industria y la secuencia de acciones tomadas por los profesionales de ciberseguridad y hacking ético para lograr los objetivos del Proyecto.
  - Descripción: muestra todas las vulnerabilidades y posibles fallas de seguridad, así como los pasos a dar para poder reproducirlas, indicando para cada una de ellas el riesgo que supone, las implicaciones que conlleva, y las amenazas y relaciones que pueda haber entre ellas.
  - Recomendaciones: para proceder a la remediación, todas ellas van acompañadas de las oportunas indicaciones para que puedan ser solventadas. En ocasiones, irán acompañadas de enlaces de páginas web externas donde obtener más información o recomendaciones adicionales para remediar o reducir los riesgos. Así como información adicional para la comprensión del riesgo existente y su posible mitigación.
  - Resultados de Ingeniería Social: descripción de los ataques de ingeniería social realizados, su tasa de éxito, y sus posibles consecuencias.

## El factor humano



Las personas son críticas. Su equipo puede resultar vulnerable y suponer un riesgo. Nuestras pruebas de Ingeniería Social son claves para identificar si los empleados necesitan capacitación en seguridad y buenas prácticas, tales como:

- Disponer de un programa de ciberseguridad y evaluar la seguridad y concienciación de los empleados y sistemas.
- Ejecutar ataques de ingeniería social como phishing, smishing, vishing o intrusiones físicas en las instalaciones que conciencien a los empleados frente a ataques reales.
- Alinear los beneficios de los test de intrusión con la mejora continua en la concienciación.

## Key Points

- Proyectos personalizados, focalizados en la revisión de los sistemas críticos del negocio.
  **Proteger los activos**
- Detallados informes conteniendo no sólo los hallazgos si no también el análisis de las causas, la forma en la que podrían ser explotados y la guía para solventarlos.
  **Combatir las amenazas**
- Resumen ejecutivo con la descripción de las vulnerabilidades y su posible impacto en las diferentes áreas de negocio.
  **Aunar esfuerzos en seguridad**
- Análisis y explotación por medio de procesos manuales siempre controlados por nuestros expertos en hacking ético.
  **Colaboración e implicación**
- Metodología orientada al análisis y testeo de los sistemas siempre dentro de la dinámica funcional de su organización
  **Pasión por nuestro trabajo**

Para más información,
contacte en el +34 933 045 600 para hablar con expertos de A2SECURE.

info@a2secure.com
www.a2secure.com

A2SECURE

A2SECURE es una empresa dedicada a la ciberseguridad. Nuestro objetivo es ayudar a prevenir y gestionar el riesgo de nuestros clientes frente a las amenazas surgidas de las comunicaciones electrónicas. Para alcanzar nuestro objetico, ofrecemos una gama de soluciones y servicios capaces de satisfacer las necesidades de nuestros clientes, adaptándose a sus requerimientos, sus recursos y disponibilidad.