HORIZON3.ai

~~TRUST BUT~~ VERIFY

Pentesting Autónomo

con Horizon3.ai

Un pentest profesional aporta valor a las organizaciones al identificar los vectores de ataque y proporcionar pruebas de explotabilidad. Puede entregar evidencia de que los controles defensivos se implementan de manera efectiva y centrar los esfuerzos de remediación en las debilidades más críticas.

Hay dos objetivos principales cuando las organizaciones realizan pentests: pentest externos para garantizar que tengan un perímetro sólido; y pentest internos para descubrir debilidades que podrían ser explotadas por un atacante que pusiera un pie dentro de la organización.

Verifique Continuamente Su Postura de Seguridad.

¿Está seguro? ¿Cómo lo sabe? No espere a que se produzca una brecha para averiguarlo. Pruebe continuamente su postura de seguridad para asegurarse de que ninguna vulnerabilidad explotable, mala configuración o credenciales apropiadas puedan dejarlo vulnerable. Los pentest externos evalúan sus activos externos para identificar cómo un adversario puede identificar y explotar las debilidades para entrar en su red.

Los pentest externos identifican vectores de ataque que incluyen:

- **Puertos abiertos y configuraciones erróneas que permiten a un atacante ingresar a la red.**
- **Vulnerabilidades sin parchar que pueden ser explotadas por usuarios no autenticados con acceso total.**
- **Proyectos TI en la sombra que aumentan la superficie de ataque.**

Presuma una Brecha para Limitar el Daño.

En el entorno actual de constantes ataques de ingeniería social por email, disponibilidad de credenciales robadas y sistemas mal configurados, las organizaciones deben suponer que ya se ha producido una brecha inicial y que los atacantes tienen un punto de apoyo en sus sistemas internos.

Un pentest interno comienza con la aceptación de que un atacante puede obtener acceso a su red interna donde residen sus datos confidenciales. Además de los vectores de ataque como los de los pentests externos, los pentest internos determinan lo que un actor malicioso puede lograr desde ese punto de partida:

- **¿Cómo pueden acceder a credenciales y privilegios adicionales?**
- **¿Qué debilidades, malas configuraciones y vulnerabilidades pueden explotar para moverse lateralmente?**
- **¿A qué datos sensibles pueden acceder?**
- **¿Exactamente qué problemas se deben arreglar y cómo – para prevenir un ataque exitoso?**

No es un Escáner de Vulnerabilidades

Los escáneres de vulnerabilidades buscan en su perímetro y sistemas internos aplicaciones sin parchar y ejecutan reglas para buscar vulnerabilidades conocidas específicas como se detalla en Vulnerabilidades y Exposiciones Comunes (CVE) del NIST. Entregan informes sobre los sistemas que "creen" que no están parchados y los CVE que pueden identificar. El ruido resultante de los problemas de baja criticidad puede distraer a los equipos para identificar y centrar el esfuerzo en las vulnerabilidades más críticas mientras se dedican ciclos a solucionar problemas no explotables.

Es importante destacar que los escáneres de vulnerabilidades no identifican los sistemas que se parcharon incorrectamente ni identifican las rutas de ataque explotables que pueden estar disponibles para los adversarios que encadenan las debilidades en sus ataques.

Vulnerable ≠ Explotable

Por el contrario, NodeZero identifica las debilidades en sus sistemas externos, locales y en la nube, así como en sus usuarios, incluso cuando los escáneres de vulnerabilidades y los sistemas de administración de parches muestran que las actualizaciones de seguridad han tenido éxito. Ofrece una ruta paso a paso y prueba de cada ataque exitoso para que los equipos entiendan cómo un atacante puede ejecutar y atacar, junto con consejos de remediación para prevenir esos ataques. Esto permite que los equipos defensivos prioricen lo que no deben arreglar para que puedan concentrarse en los problemas más críticos que afectan a su posturas de seguridad sin desperdiciar ciclos en problemas no explotables.

NodeZero

Verifique continuamente su postura de seguridad
NodeZero soluciona el problema de pentest caros automatizando el proceso.
NodeZero es una solución de pentesting autónomo – como "autoservicio", que es seguro de correr en producción, analiza los sistemas como lo haría un pentester manual pero más rápido, más completo, y con más resultados accionables.

~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

HORIZON3.ai
~~TRUST BUT~~ VERIFY

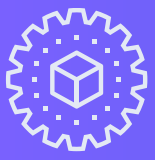
Que es un Pentest Autónomo?

NodeZero es diferente a otras soluciones de pentesting: combina las capacidades de prueba de alta frecuencia y menor costo de las pruebas de pentesting automatizadas con la experiencia, minuciosidad y precisión de las pruebas de pentesting manuales realizadas por profesionales de seguridad altamente calificados. El resultado es la capacidad de ejecutar ejercicios continuos de formación de equipos morados a un bajo costo anual. El Pentesting ha evolucionado de manual, a colaborativo, a automatizado, y ahora autónomo.

El pentesting manual requiere un recurso de seguridad capacitado que utilice herramientas comerciales y especializadas para explorar una aplicación o sistema e identificar debilidades. La efectividad (y el costo) de un pentest manual depende del tiempo asignado a la prueba y la habilidad del pentester, lo que lleva a muchas organizaciones a ahorrar costos y proporcionar credenciales a los pentesters. Si bien los resultados son mucho más limpios que en un pentest automatizado, los consejos de remediación a menudo son limitados. Además, el alto costo de las pruebas de penetración manuales impide que las organizaciones las usen con frecuencia, como después de que un sistema es parchado y asegurarse que quedó bien actualizado.

El pentesting automatizado es un simple enfoque “point and click” usando herramientas comerciales de análisis dinámico. La herramienta recibe una URL o dirección IP y analiza la aplicación para identificar campos donde un hacker podría ingresar datos. La herramienta “ingresa” datos a los campos para intentar probar debilidades en la validación que podrían ser explotadas por un hacker avezado o abrumar la aplicación con un ataque de denegación de servicio. Estas pruebas normalmente se ejecutan en 1 ó 2 días y generan mucho “ruido”; resultados no probados que los defensores deben investigar para determinar si requiere remediación.

El pentesting colaborativo incluye pentests manuales, y se basa en una red de investigadores independientes de seguridad que reciben un pago “por vulnerabilidad identificada” (más un pago por plataforma para el proveedor). Los pentests colaborativos tienen la ventaja de ser abiertos, es decir – en teoría – puede tener gente buscando problemas todos los días, durante meses. Pueden ser caros si hay un gran número de vulnerabilidades, y los hallazgos a menudo no tienen como probar explotabilidad haciendo que los desarrolladores gasten tiempo en problemas que no son críticos.



El pentesting autónomo combina los beneficios del pentesting automatizado; pruebas más frecuentes, costos menores, y sin necesidades de experiencia interna de seguridad, con las de pentests manuales; cobertura más completa de la aplicación y explotabilidad probada. El pentesting autónomo no necesita credenciales para comenzar. Puede encadenar debilidades como un hacker avanzado y automáticamente generar ataques para aislar la causa basal de un ataque. Esto permite a los defensores entender exactamente qué cambios se necesitan hacer para proteger una aplicación.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Cómo Funciona NodeZero

Reconocimiento

Todo ataque exitoso requiere inteligencia sobre el objetivo. NodeZero comienza con acceso no autenticado al sistema, y crea un Gráfico de Conocimiento, identificando todos los hosts, malas configuraciones, puertos abiertos, y busca credenciales.

Loop de Maniobras

NodeZero orquesta más de 100 herramientas ofensivas para apropiarse de credenciales, explotar vulnerabilidades, y aprovecharse de valores por defecto y malas configuraciones para ejecutar ataques.

Planes de Ataque Verificados

Para simplificar la priorización y remediación los resultados se entregan como “Pruebas” con representaciones gráficas y textuales de cada paso de un ataque exitoso. Esto incluye cuales tácticas fueron usadas, cuales debilidades fueron identificadas y atacadas, cómo se obtuvieron credenciales, y las rutas seguidas para obtener privilegios y acceder a los sistemas.

Impacto

NodeZero identifica e informa sobre datos en riesgo en ambiente físico y virtual a los que pudo acceder con privilegios de read/write, incluyendo compartidos SMB, NFS, FTP, cloud storage, servidores vCenter, y bases de datos.

Evaluación Contextual

NodeZero evalúa y prioriza cada debilidad por su rol en un ataque exitoso – no en base a la puntuación CVSS. Las organizaciones pueden identificar rápidamente las debilidades que son una amenaza y deben ser tratadas inmediatamente, y cuáles pueden ser diferidas sin correr riesgos.

Remediación Accionable

NodeZero proporciona una guía de remediación precisa y procesable, lo que permite a seguridad y operaciones resolver rápidamente los problemas en la causa raíz.

¿Listo para aprender más?

NodeZero es un pentest autónomo como servicio (APTaaS) que ayuda a las organizaciones a encontrar y corregir los vectores de ataque antes de que los atacantes puedan explotarlos. Es seguro ejecutarlo en producción y no requiere agentes persistentes o

- **Solicite su demo gratis hoy mismo.**
  https://horizon3.ai/demo

HORIZON3.ai
TRUST BUT VERIFY