LA EVOLUCION DEL PENETRATION TESTING

En Synergy nuestro objetivo es prevenir amenazas y gestionar el riesgo tecnológico garantizando el cumplimiento con los estándares internacionales y las mejores prácticas de seguridad.

Contamos con un fuerte enfoque técnico que nos permite detectar vulnerabilidades en aplicativos web, mobile, APIs y servicios de red.

REPORTES INTELIGENTES

Todos los hallazgos de seguridad se entregan a través de una moderna plataforma SaaS. Cada vulnerabilidad se presenta con descripciones claras y recomendaciones por parte de nuestros especialistas enfocadas en hacer que las cosas sean inmediatamente procesables para usted.

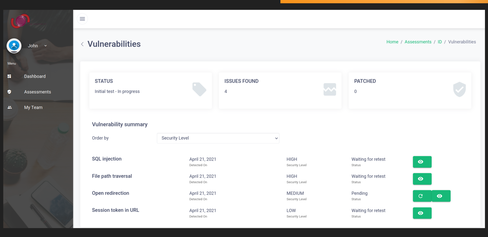
Acceda a los hallazgos y recomendaciones en tiempo real en lugar de esperar un informe PDF estático con un precio excesivo. Nuestra plataforma le permite solicitar la validación de los parches implementados con solo un click, incluso si la prueba de penetración no ha finalizado.

Los informes en PDF están disponibles en caso de que necesite compartirlos con sectores internos, socios comerciales, auditores u otras entidades externas.

Hallazgos en tiempo real:
Acceda a las vulnerabilidades inmediatamente luego de ser detectadas.

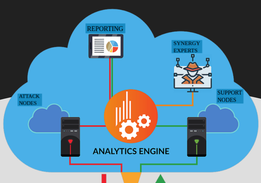
Retesting ilimitado:
La repetición de pruebas está incluida y gestionada por el mismo equipo de pentesters que descubrió los hallazgos para garantizar la coherencia de las mismas.

Cumplimiento con estándares:
Cumpla con los requisitos de pruebas de penetración para certificaciones como PCI DSS, ISO 27001, SOC2 y HITRUST.



ENFOQUE BASADO EN LA NUBE

A diferencia de los servicios de pruebas de penetración convencionales, aprovechamos nuestra propia botnet para realizar pruebas de seguridad. Esto nos permite expandir la superficie de ataque y descubrir fallas de seguridad rápidamente mientras mantenemos precios altamente competitivos. Esta metodología es útil para evitar diferentes tipos de medidas de bloqueo de IP, como la protección por fuerza bruta, la limitación de velocidad basada en IP o listas negras de IP basadas en WAF.



Reportes inteligentes:
Este proceso ocurre simultáneamente con los otros tres. Documenta y entrega al cliente todos los hallazgos al mismo tiempo que son detectados, evitando perder tiempo al finalizar el análisis de las pruebas de penetración.

Expertos de Synergy:
Nuestros testers de penetración gestionan la botnet coordinando el análisis, creando tareas específicas y evaluando el resultado de cada ataque.

Attack nodes:
Un nodo de ataque es donde se generan todas nuestras conexiones al servidor de destino. Utilizamos un grupo de este tipo de nodos para realizar ataques orquestados.

TARGET

Support nodes:
Los nodos de soporte proporcionan detección pasiva a nuestra solución. También ayudan a descubrir varios tipos de vulnerabilidades de conexión inversa. Por ejemplo, algunas vulnerabilidades basadas en inyecciones se pueden detectar utilizando cargas útiles que desencadenan una interacción con un sistema externo cuando se produce una inyección exitosa, aquí es cuando entran en juego nuestros nodos de soporte.

SERVICIOS DE PRUEBAS DE SEGURIDAD

Web Application Penetration Testing

El equipo de testers de penetración de aplicaciones web de Synergy evalúa su plataforma web contra OWASP Top 10 y CWE / SANS Top 25 a través de una combinación de pruebas manuales y automatizadas. Si su aplicación está alojada en un entorno de nube, Yappo también analiza todos los servicios de nube relacionados con la plataforma.

API Penetration Testing

Una API mal protegida puede abrir brechas de seguridad para cualquier sistema con la que esté asociada. Permita que Synergy lo ayude a evaluar su API de SOAP y REST contra el estándar OWASP API Security Top 10 y mediante la realización de escenarios de prueba complejos de autenticación, cifrado y control de acceso.

Mobile Penetration Testing

Basándose en la metodología OWASP Mobile Top 10 que incluye las fallas de seguridad más peligrosas de las aplicaciones móviles, los testers de penetración de Synergy analizan las aplicaciones IOS y Android para asegurarse de que su solución esté segura en el mercado.

Network Penetration Testing

El equipo de Synergy intenta ingresar a su sistema para evaluar su nivel de madurez de seguridad. Este análisis le permite identificar vulnerabilidades de seguridad que podrían ser explotadas por un atacante remoto para poner en peligro sus sistemas. Conozca que visibilidad tiene un hacker de su entorno externo.

ELIJA EL MEJOR TIPO DE PRUEBA PARA USTED

La cantidad de información compartida antes de un compromiso puede tener una gran influencia en sus resultados. El estilo de prueba generalmente se define como prueba anónima o autenticada.

Prueba Anónima

- Usuario no autenticado
- Análisis en capas de aplicación y sistema
- Múltiples escaneres
- Verificación manual

Prueba Autenticada

- Usuario autenticado por cada rol
- Procesos automatizados y manuales
- Elevación de privilegios
- Análisis en funciones restringidas
- Verificación manual

PENTESTING PARA CUMPLIMIENTO

Nuestros servicios brindan cobertura PCI DSS, GDPR y HIPAA para pruebas de seguridad.

Requerimientos de pruebas de seguridad en GDPR

Los "Principios de seguridad" en el artículo 5(1)(f) de GDPR dice que los datos personales deben ser: "Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

Requerimientos de pruebas de seguridad en PCI DSS

- Requerimiento PCI DSS 6.1 – Puede cumplirse mediante el establecimiento de un proceso para identificar vulnerabilidades de seguridad en sus aplicaciones internas y externas, mediante el uso de fuentes externas acreditadas para obtener información sobre vulnerabilidades de seguridad, y asignando una clasificación de riesgo (por ejemplo, como 'alto', 'medio' o 'bajo') a vulnerabilidades de seguridad recién descubiertas.

- Requerimiento PCI DSS 11.3.1 – Cubre la necesidad de realizar pruebas de penetración externas al menos una vez cada seis meses y después de cualquier cambio significativo o actualización de la infraestructura o aplicación de la organización.

- Requerimiento PCI DSS 11.3.3 – Dice que las vulnerabilidades encontradas durante las pruebas de penetración deben resolverse y se deben realizar pruebas adicionales hasta que las vulnerabilidades se aborden adecuadamente.

Requerimientos de pruebas de seguridad en HIPAA

- Aunque HIPAA no requiere una prueba de penetración o un escaneo de vulnerabilidades, el análisis de riesgo es una parte integral del proceso de cumplimiento de HIPAA.

- El cumplimiento de HIPAA requiere que las entidades cubiertas prueben sus controles de seguridad de forma regular.

NUESTRA HISTORIA Y VALORES

Synergy nace como una iniciativa de un grupo de profesionales en el campo de la seguridad de la información, con más de 10 años de experiencia en el mundo TI y seguridad ofensiva.

Cada miembro de nuestro equipo ha trabajado en empresas de diversos tamaños, por lo que entendemos la necesidad y disponibilidad de cada tipo de negocio.

Mantenemos relaciones a largo plazo con cada uno de nuestros clientes, estableciendo confianza mutua y convirtiéndonos en su principal socio de ciberseguridad. Para lograrlo, creamos valor agregado a nuestros servicios y buscamos la máxima predisposición por parte de cada uno de nuestros miembros.