ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Servicio de **Auditoría Interna de Redes y Sistemas** *(Hacking Ético)*

RETOS

Las PYMEs se enfrentan a una serie de complejos desafíos, azuzados por un mercado tremendamente ágil y en constante evolución. Desde la incertidumbre económica hasta la competencia feroz, las PYMEs deben adaptarse a las cambiantes tendencias y a la rápida evolución de la tecnología, manteniéndose actualizadas y flexibles para garantizar la relevancia de sus productos y servicios. La digitalización también está poniendo de manifiesto el crecimiento de la superficie de ataque, aumentando así las posibilidades de sufrir un ciberincidente con las consecuencias que ello puede conllevar para su supervivencia.

CIFRAS CLAVE

- El **83%** de las **PYMEs no están preparadas** para responder ante un **ciberataque**.
- El **30%** de las **PYMEs** teme al **phishing** como una de sus principales **ciberamenazas**.
- El **91%** de las **PYMEs** aún no cuenta con un **ciberseguro de responsabilidad.**

SOLUCIONES

Conocemos profundamente las necesidades de las PYMEs, y tratamos de darles cumplimiento diseñando, implantando, manteniendo y operando planes integrales de seguridad basados en las seis funciones del NIST (Gobierno, Identificación, Protección, Detección, Respuesta y Recuperación). Dentro de ellas, nuestro servicio *de Auditoría Interna* le permitirá obtener luz sobre la resiliencia de su red interna, entendiendo cuáles son sus principales carencias para poder corregirlas a la mayor brevedad.

¿Cómo evaluamos la madurez de una red interna?

Nuestras Auditorías Internas se basan en cinco fases principales:

- Recopilación de información.
- Análisis de vulnerabilidades de infraestructura.
- Análisis de vulnerabilidades de aplicaciones y servicios.
- Recopilación de evidencias.
- Redacción del informe.

Desde Zerolynx se ha elaborado una metodología propia basada en los mejores estándares del mercado, como PTES, OSSTMM y OWASP. Esta metodología establece las pautas para la realización de pruebas de intrusión y búsqueda de vulnerabilidades sobre auditorias de seguridad interna, detallando cómo realizar la comprobación de cada vulnerabilidad.

SOBRE GRUPO ZEROLYNX

Proveedor europeo de Ciberseguridad e Inteligencia.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE

ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Servicio de **Auditoría Interna de Redes y Sistemas** *(Hacking Ético)*

Dentro de la metodología planteada, son destacadas las siguientes pruebas:

Análisis del endpoint

- Cifrado de disco.
- Contraseñas seguras.
- Políticas seguras (acceso a powershell, tiempo de cierre de sesión, etc.).
- Escalada de privilegios local.

Ataques en la red

- Arp Spoofing – MiTM.
- Comunicaciones cifradas.
- Segmentación de redes.
- Protocolos inseguros.
- Credenciales por defecto en electrónica de red (switches, firewalls, routers).
- Acceso a red Tor.
- Exfiltración de datos (evasión de firewall, proxies, etc.).
- Pruebas de phishing (pendrive infectado, emails fraudulentos, Rogue AP, etc.).

Análisis de vulnerabilidades en el software

- Software sin soporte y/o desactualizado.
- Vulnerabilidades en el software instalado.
- Credenciales por defecto en servicios.

Pruebas de Malware

- Detección de malware.
- Acceso a sitios potencialmente peligrosos.
- Bypass de antivirus/EDR.
- Ejecución y beaconing C&C.

Análisis de Directorio Activo

- Análisis de relaciones en Directorio Activo.
- Análisis de camino más corto a administrador de dominio.
- Movimientos horizontales y verticales en la organización (sysvol, golden ticket, pass-the-hash, etc.).
- Volcado de credenciales.

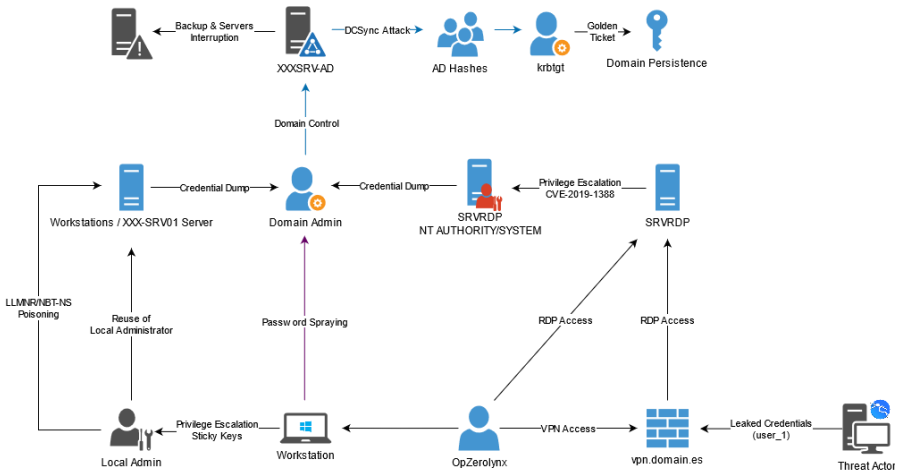
info@zerolynx.com
info@osaneconsulting.com

ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Servicio de **Auditoría Interna de Redes y Sistemas** *(Hacking Ético)*

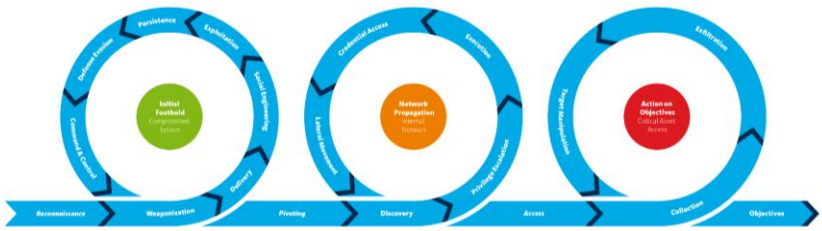
Killchain

Zerolynx siempre incluye un gráfico que detalla todas las vías de compromiso obtenidas en el entorno del cliente, obtenidas durante la ejecución del proyecto para la consecución de objetivos principales o secundarios. Este gráfico detalla las diferentes vías de ataque existentes que un actor malicioso habría podido seguir con el objetivo de alcanzar su misión dentro de la organización.



DOMAIN.ES

Junto a este gráfico se añade una descripción textual de las vías de ataque y el impacto que cada uno de estos escenarios habrían tenido sobre la compañía, y que sirve como resumen de alto nivel de los escenarios logrados durante el ejercicio.



Las diferentes actividades realizadas se enmarcarán dentro de la *Cyber Kill Chain*, con el objetivo de localizar las deficiencias detectadas en las diferentes etapas del ciclo de vida del ataque de los actores maliciosos.

CYBERSECURITY & INTELLIGENCE

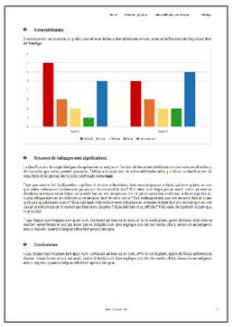
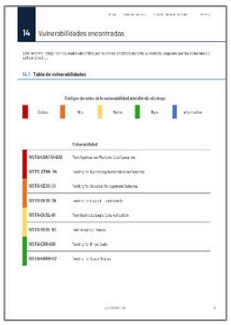
Servicio de **Auditoría Interna de Redes y Sistemas** *(Hacking Ético)*

Informe final

Mediante la consolidación de todas las evidencias obtenidas se construirá un completo informe técnico y ejecutivo de acuerdo con el modelo de Zerolynx, e incluirá, al menos, los siguientes puntos:

- Objeto y alcance de la auditoría
- Sistemas auditados
- Equipo auditor
- Interlocutores que hayan intervenido en la auditoría
- Fechas de desarrollo de las pruebas
- Documentación de referencia
- Cláusula de confidencialidad
- Vulnerabilidades detectadas, clasificadas según su importancia
- Soluciones recomendadas a las vulnerabilidades
- Vulnerabilidades subsanadas en la auditoría
- Observaciones
- Puntos fuertes y oportunidades de mejora
- Conclusiones obtenidas

El informe contará con un Resumen Ejecutivo, resaltando los principales riesgos detectados y recomendaciones de priorización para su posible resolución. A continuación, se muestran ejemplos de resumen ejecutivo y fichas de vulnerabilidad usadas por Zerolynx. No obstante, la información del informe y las vulnerabilidades se podrá adaptar a las necesidades y requerimientos del cliente si así fuera necesario.

Asimismo, Zerolynx pone a disposición del cliente una presentación a alto nivel al final del proyecto en la que se documentarán los principales hallazgos y remediaciones.