PROPUESTA EJECUTIVA Y ECONÓMICA

Servicio de Pentesting Empresarial

Diseñado para CISO, Gerencia de IT y equipos responsables de proteger la infraestructura, aplicaciones y activos críticos de la organización.

Objetivo Identificar vulnerabilidades explotables antes de que impacten continuidad, datos o reputación.	**Cobertura** Infraestructura interna, Active Directory, servidores web, APIs, cloud y aplicaciones in-house.
Metodología Enfoque alineado con OWASP, PTES y buenas prácticas de validación manual.	**Valor ejecutivo** Reporte para dirección, backlog priorizado para IT y re-test para validar cierres.

Formato Evaluación puntual o programa recurrente	**Modalidad** Black Box, Grey Box o White Box	**Entrega** Reporte ejecutivo + técnico + re-test

1. Resumen ejecutivo

El servicio de pentesting permite validar, con una perspectiva de atacante real, si la organización presenta brechas que puedan ser utilizadas para comprometer disponibilidad, confidencialidad o integridad. El foco no es solo detectar hallazgos; es demostrar impacto, priorizar la remediación y traducir el riesgo técnico en decisiones accionables para negocio y IT.

Resultados esperados

- Visibilidad sobre exposición real de la superficie evaluada.
- Priorización de vulnerabilidades por severidad e impacto de negocio.
- Hoja de ruta de remediación con quick wins y acciones estructurales.
- Validación posterior mediante re-test.

2. Alcance sugerido

Módulo	Qué se evalúa	Herramientas y enfoque
Infraestructura interna	Escaneo de red, enumeración de servicios, segmentación, shares, exposición y rutas de movimiento lateral.	Nmap, Netdiscover, arp-scan, enum4linux-ng, SMB/RPC/LDAP review.
Active Directory	Identificación de debilidades en autenticación, privilegios, delegaciones y relaciones de confianza.	BloodHound, CrackMapExec/NetExec, Impacket, Kerberos testing.
Servidores web y APIs	Validación de autenticación, autorización, inyecciones, manejo de sesión y lógica de negocio.	Burp Suite, OWASP ZAP, Nuclei, ffuf, sqlmap, revisión manual.
Apps in-house	Análisis estático y dinámico, decompilación, secretos, endpoints y mecanismos de almacenamiento.	JADX, apktool, Ghidra, MobSF, Frida, revisión de binarios y strings.
Cloud y configuración	Revisión de exposición pública, malas configuraciones y privilegios excesivos.	Prowler, ScoutSuite, AWS/Azure/GCP CLI, validación de IAM.

3. Metodología de ejecución

Fase	Bloque	Descripción
1	**Scoping**	Definición de alcance, exclusiones, ventanas de prueba y reglas de engagement.
2	**Reconocimiento**	Mapeo de superficie, descubrimiento de activos, dominios, servicios y tecnologías.

3	**Enumeración**	Identificación de versiones, shares, endpoints, permisos y flujos de autenticación.
4	**Explotación controlada**	Prueba de vectores explotables con validación manual y mínima afectación operativa.
5	**Post-explotación**	Evaluación de privilegios, movimiento lateral, exposición de datos e impacto real.
6	**Reporte y re-test**	Entrega ejecutiva, plan de remediación y validación posterior de correcciones.

4. Entregables

Reporte ejecutivo Resumen para dirección con riesgo global, top hallazgos, impacto y priorización.	**Reporte técnico** Detalle por vulnerabilidad con evidencia, reproduccción, severidad y recomendación.
Matriz de remediación Backlog priorizado para IT con acciones inmediatas, altas, medias y planificadas.	**Re-test** Validación formal de remediaciones y actualización de estado de hallazgos.

5. Paquetes comerciales de referencia

Plan	Cobertura	Tiempo estimado	Entregables incluidos	Inversión referencial
Starter	1 vector de prueba o alcance acotado	1-2 semanas	Reporte ejecutivo, técnico y re-test acotado	**Desde USD 4,500**
Professional	Multi-vector, mayor profundidad manual	2-4 semanas	Todo Starter + workshop de remediación	**Desde USD 9,500**
Enterprise	AD, web, APIs, cloud y apps in-house	4+ semanas	Todo Professional + comité ejecutivo y roadmap 30/60/90	**A medida**

Nota: los valores son referenciales y pueden ajustarse según cantidad de activos, criticidad, profundidad requerida, ventanas de prueba y necesidad de re-test ampliado.

6. Siguientes pasos

- Alinear alcance y supuestos en una sesión de 30-45 minutos.
- Definir activos incluidos, exclusiones y ventana operativa.
- Emitir propuesta final y Statement of Work (SOW).
- Iniciar ejecución y entregar hallazgos priorizados según cronograma acordado.