Ethical Hacking

COSIM
22 años en CiberSeguridad

Servicio para Análisis de Vulnerabilidades Técnicas a través de Pruebas de Intrusión

Gestión de Vulnerabilidades

Un test de intrusión consiste en simular un ataque a una red o sistema para evaluar el perfil de riesgo de un entorno, utilizando las mismas técnicas y herramientas que un hacker (ciberatacante).
Sus objetivos son los siguientes:

- Identificar los activos de información desde los diferentes vectores de ataque.
- Analizar errores de configuración y debilidades de los controles tecnológicos.
- Determinar la efectividad de los controles técnicos.
- Verificar si las vulnerabilidades identificadas son potencialmente explotables.
- Clasificar las vulnerabilidades según su nivel de riesgo técnico.
- Recomendar contramedidas específicas para una remediación efectiva de las vulnerabilidades.
- Brindar información ejecutiva para la toma de decisiones gerenciales.

Prueba de Intrusión

La clave para un Pen Test satisfactorio y valorable es tener claramente definidos los objetivos, alcance, metas señaladas, limitaciones, y actividades aceptables. Este alcance es definido por un análisis de riesgo previamente realizado sobre los procesos de negocio más relevantes para la organización y aprobado por la gerencia propietaria del negocio.

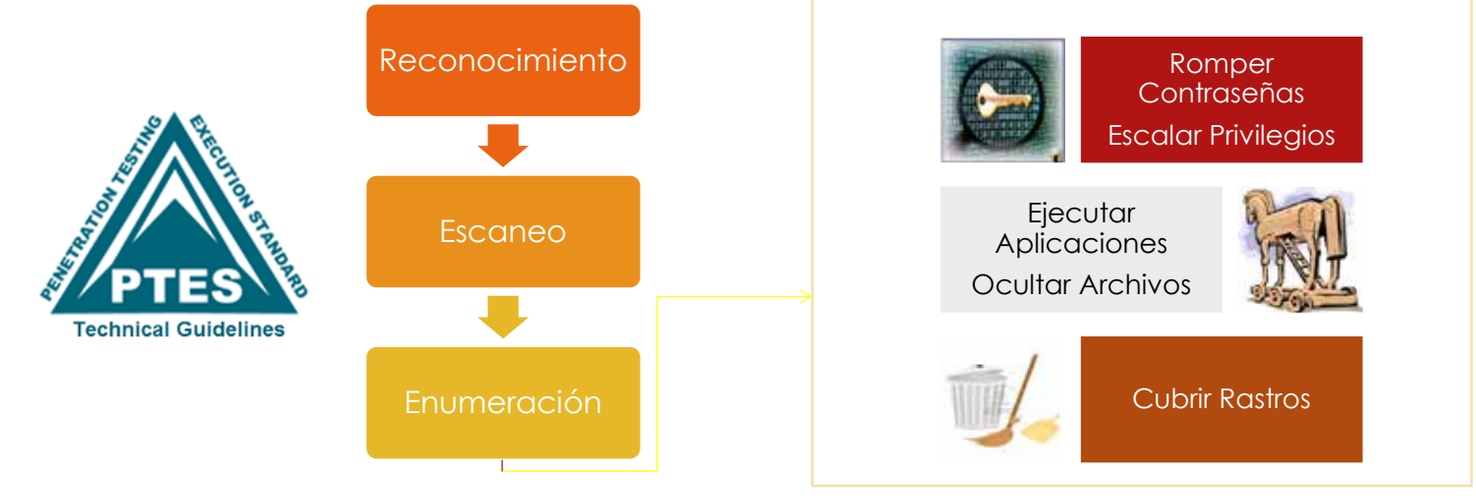
COSIM, pentest en el sector petrolero y financiero

Nuestro personal designado realiza todo el año específicamente servicios de ethical hacking para diferentes empresas y entornos, desde pruebas de intrusión a redes corporativas, hasta análisis estático y dinámico de aplicaciones web y móviles (Banca transaccional), análisis de vulnerabildades en sistemas industriales DCS/SCADA y pruebas de seguridad sobre cajeros automáticos (ATMs).

Metodología para Pruebas de Intrusión

Si bien existen diversas metodologías para ejecutar pruebas de intrusión controladas, COSIM se apoya en la combinación de las metodologías internacionales más aceptadas en la industria de seguridad ofensiva, como ser; PTES (*Penetration Test Execution Standard*) y la metodología OWASP para el testeo de aplicaciones, tanto móviles como web o de escritorio.

PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines



Por qué COSIM?

1. Más de 22 años respaldan nuestra experiencia en Ciberseguridad y pruebas de intrusión.
2. Primera empresa boliviana en contar con personal dedicado especificamente a pentest.
3. Conocimiento sólido del rubro petrolero y financiero de Bolivia y la sensibilidad de sus sitemas.
4. Más de 100 servicios exclusivamente de pentest realizados a la fecha.
5. La empresa boliviana con más pentesters certificados por Offensive Security (4 recursos).
6. Experiencia comprobada en pentest de sistemas críticos DCS/SCADA.
7. Nuestros pentesters senior son empleados de planilla, COSIM no trabaja con freelancers.
8. Nuestro personal se encuentra certificado en las herramientas que emplea, como ej. KALI Linux.
9. Cada servicio es gestionado como proyecto, para el cumplimiento de alcance, tiempo y calidad.
10. Solvencia y seriedad para el manejo reservado de la información confidencial de la entidad cliente.

Amenazas emergentes

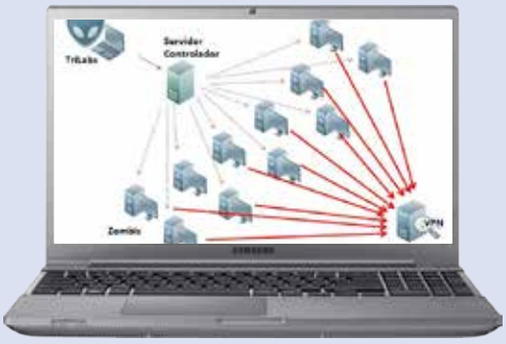
Durante la pandemia y confinamiento incrementaron las amenazas a los siguientes recursos y servicios de negocio:

- VPNs de Teletrabajo
- Apertura de cuentas on-line
- Servicios de habilitación (de opciones) de banca web/móvil vía internet
- Servicio de desbloqueo de cuentas de banca por internet
- Empleados incautos (correos frauduentos tipo phishing tratando de obtener sus credenciales de acceso a la VPN y servicios en la nube.

Características principales

Alcance.- Más allá de las pruebas a la red interna y pruebas externas a la red perimetral y sitios web, es necesario testear las conexiones VPN de teletrabajo en caso de estar habilitada esta modalidad.

Las pruebas de tipo DoS deben ser coordinadas por escrito y controladas entre ambas partes.



Web App Hacking.- La dinámica de los negocios en entidades financieras exige un desarrollo de aplicaciones (sobretodo web y móvil) así como un mantenimiento permanente de las mismas, lo cual conlleva serios riesgos de seguridad si estas no son testeadas antes de su habilitación en ambiente productivo.

COSIM cuenta con especialistas en testeo de aplicaciones web y móviles, lo cual exige un perfil dedicado a este ramo de la ciberseguridad

Capacidades principales

Experiencia.- Nuestro personal cuenta con experiencia realizando pruebas de Ethical Hacking dentro y fuera del país, testeando aplicaciones web y móviles para diferentes entidades financieras de latinoamerica.

Asimismo, realizando cursos y talleres en múltiples países como México, Brasil, Perú y Paraguay.

Personal Certificado.- Nuestros pentesters se encuentran certificados internacionalmente en seguridad ofensiva y hacking ético, emitidas por Offensive Security:

- OSCE (Offensive Security Certified Expert)
- OSCP (Offensive Security Certified Professional)
- OSWP (Offensive Security Wireless Professional).

A la fecha COSIM es la empresa con más recursos certificados por esta organización israelí.

Herramientas.- Suite de Kali Linux (Nmap, ncat, DNSEnum, Metasploit, entre otros según los resultados parciales de las pruebas) además de dispositivos de ataque: Pineapple Wifi, Rubber Ducky, Lan Turtle, keyloggers, entre otros.

Asimismo, COSIM es partner de Tenable (escaner de vulnerabilidades Nessus).

Entregables.- Entre los principales se encuentran:

- **Informe Gerencial**, resumen ejecutivo de los hallazgos, expresado en gráficos y datos porcentuales.

- **Informe Técnico**, detallando el trabajo realizad, pantallazos de ejemplo, entre otros detalles.

- **Matriz de vulnerabilidades técnicas**, relacionada al informe técnico, con las contramedidas específicas para la remediación de vulnerabilidades. Documento base para el **plan de acción**.

Los ataques ocurren porque las vulnerabilidades no son abordadas y solucionadas a tiempo. La gestión de vulnerabilidades técnicas consiste en que el proceso de identificación, categorización y remediación de vulnerabilidades sea recurrente más allá de los servicios contratados de Ethical Hacking.

Israel Rosales
Gerente de Proyectos
COSIM TI SRL