



**INFORME TECNICO PREVIO DE EVALUACION DE
SOFTWARE N° 007-2010-2A2000**

1. NOMBRE DEL AREA:

Oficina de Investigación Tecnológica

2. RESPONSABLES DE LA EVALUACION:

Ernesto Arévalo Arrascue

3. CARGO:

Profesional Especializado I

FECHA

20 de septiembre del 2010

5. JUSTIFICACIÓN

La Oficina de Seguridad Informática solicita la adquisición de una herramienta de test de intrusión que permita a los profesionales de seguridad informática ejecutar acciones para identificar y corregir vulnerabilidades que puedan ser empleadas para una intrusión no autorizada a la plataforma informática de la Institución. Estas acciones de aseguramiento permitirán incrementar los niveles de seguridad de los servicios informáticos y transacciones electrónicas que presta la Institución a los Contribuyentes y Operadores de Comercio Exterior a través de la plataforma informática y el portal web (www.sunat.gob.pe).

6. ALTERNATIVAS

En la exploración tecnológica del mercado se analizaron las siguientes herramientas que cuentan con representación y soporte local:



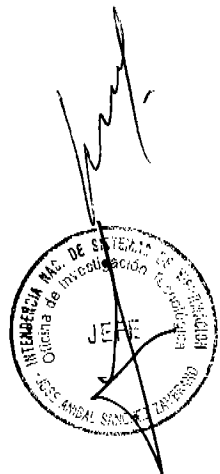
Herramientas de Test de Intrusión (Penetration testing)

- Core Impact pro.
- Saint Exploit.
- Immunity Canvas.

7. ANALISIS COMPARATIVO TECNICO

Para cada uno de los productos seleccionados se han evaluado los atributos mínimos que la solución debe contemplar, en el siguiente cuadro se muestran los puntajes de cada atributo:

	Puntaje Max. 100 ptos.	Core Impact	Saint Exploit	Immunity Canvas
ATRIBUTOS INTERNOS	40	40	40	40
Funcionalidad: Interoperatividad El software debe ser compatible con el hardware ofertado y debe permitir realizar un test de penetración sobre un rango mínimo de 250 dispositivos.	10	10	10	10
Funcionalidad: Adecuación El software debe ser capaz de permitir realizar una secuencia de ataques, desde la obtención de la información, hasta la ejecución y explotación de la vulnerabilidad y del ataque.	10	10	10	10
Funcionalidad: Exactitud Debe identificar vulnerabilidades sobre los diferentes recursos informáticos de la Red.	10	10	10	10
Funcionalidad: Exactitud Debe contar con exploits que permitan probar si la vulnerabilidad detectada es un riesgo alto de seguridad para la red.	10	10	10	10
ATRIBUTOS EXTERNOS	30	30	30	30
Funcionalidad: Interoperatividad Debe instalar un agente en un equipo comprometido y permitir ejecutar adicionales ataques desde ese equipo.	10	10	10	10
Funcionalidad: Exactitud Debe incluir la generación de reportes de los resultados.	10	10	10	10
Capacidad de Mantenimiento: Conformidad de la facilidad de mantenimiento. Soporte directo del fabricante.	10	10	10	10



ATRIBUTOS DE USO	30	30	30	30
Productividad Debe permitir crear macros, para automatizar tareas.	6	6	6	6
Productividad Pruebas de intrusión para identificar deficiencias en aplicaciones web, web servers y bases de datos asociadas.	6	6	6	6
Productividad Pruebas de intrusión para servidores y estaciones de trabajo, servidores y servicios de seguridad (Antivirus, anti-phishing, anti-malware, IPS/IDS y otros).	6	6	6	6
Productividad Pruebas de intrusión contra redes wireless.	6	6	6	6
Eficacia Identificar vulnerabilidades que permitan acceso no autorizado a la red.	6	6	6	6
PUNTAJE TOTAL	100	100	100	100

Del análisis técnico de las características y funcionalidades, las tres herramientas cumplen con las características mínimas requeridas.

8. ANALISIS COMPARATIVO DE COSTOS


Los costos de cada herramienta se muestran en cuadro adjunto:

HERRAMIENTA TEST DE INTRUSION	CORE IMPACT	SAINT EXPLOIT	IMMUNITY CANVAS
Provisión, instalación, configuración, puesta en producción, capacitación. Incluye Hardware.	84,567.00	126,186.24	65,577.70
Garantía de buen funcionamiento, mantenimiento y soporte de la herramienta 3 años.	36,243.00	55,561.11	54,853.50
TOTAL Nuevos Soles S/. inc. IGV	120,810.00	181,747.35	120,431.20

9. CONCLUSION

Las tres herramientas analizadas cumplen con los requisitos mínimos requeridos. Por tanto se recomienda realizar un proceso de adquisición por concurso en la que participen las herramientas evaluadas además de cualquier otra herramienta que satisfaga los requerimientos mínimos exigidos.

10. FIRMAS

JOSE ANIBAL SANCHEZ ZAMBRANO
Jefe de la Oficina de Investigación Tecnológica
INTENDENCIA LOCAL DE LOS SISTEMAS DE INFORMACION