PR-CIB-001

PRUEBAS DE PENETRACION

Responsables

Elaboró:	Líder de Servicios de Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Dirección General

Control de versiones

Versión	Fecha	Descripción del cambio
1	28/02/19	Emisión inicial
2	27/05/19	Se actualiza diagrama de flujo derivado de los hallazgos generados en la auditoría interna del SGI.
3	02/10/2019	Actualización del procedimiento de acuerdo a los hallazgos de auditoría interna.
4	20/09/2022	Actualización de formato y revisión general del documento

Contenido

1. Objetivo del procedimiento 3
2. Alcance 3
3. Definiciones 3
4. Responsabilidades 3
5. Descripción de actividades 4
6. Documentos relacionados 6
7. Anexos 6

1. Objetivo del procedimiento

Establecer las actividades a seguir para la ejecución del servicio de "pruebas de penetración" a diversos componentes informáticos, mediante herramientas de software, técnicas manuales, y desarrollo de actividades apegadas a metodologías líderes y buenas prácticas relacionadas al servicio, con la finalidad de determinar la debilidades o fortalezas ante el conjunto de amenazas conocidas al día de la evaluación tanto para elementos externos e internos, detectando oportunidades de mejora para proteger la infraestructura y diversos activos de una organización.

2. Alcance

Aplica para los servicios de Pruebas de Penetración de acuerdo con los requerimientos de los Clientes.

3. Definiciones

Pruebas de penetración (también llamadas "pen testing"): Son una práctica para evaluar la seguridad de un sistema informático, red, aplicación o algún activo para encontrar vulnerabilidades que un atacante podría explotar.

Pruebas de caja negra: Revisión de seguridad en la cual los consultores asignados a la revisión cuentan con la mínima información sobre los activos bajo alcance.

4. Responsabilidades

Rol	Responsabilidades y/o funciones
Líder de Servicios de Ciberinteligencia:	•Realizar la presentación de Kick Off a nivel de ejecución de este como: alcance, puntos de contacto, cronograma, puntos de comunicación, corroborar alcance. •Revisa los informes entre pares
Entrega de Servicios:	Revisar la presentación del Kick Off así como validar los entregables antes de liberación a cliente.
Cliente:	Confirmar componentes del servicio, así como alcance, recibir entregables y firmar de conformidad.
Especialista de Ciberinteligencia	Realizar actividades de reconocimiento de los activos definidos en el alcance, realizar el análisis de vulnerabilidades y actividades de Post-explotación de acuerdo con el alcance de la fase.

5. Descripción de actividades

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Validar el alcance	Líder de ciberinteligencia	Validar el alcance de acuerdo con el servicio solicitado	NA
2.	Revisar si se requiere presentación de kick off	Líder de ciberinteligencia	Revisar si se requiere presentación de kick off, de acuerdo a los requerimientos del servicio solicitado ¿Se requiere presentación? Si: Continuar con la actividad 3. No: Continuar con la actividad 5.	NA
3.	Realizar la presentación de Kick Off	Líder de ciberinteligencia	Presentación de los diferentes componentes del servicio a nivel de ejecución de este como pudiera ser: alcance, puntos de contacto, cronograma, puntos de comunicación, entre otros	Presentación Kick Off
4.	Participar en la reunión de Kick Off	Cliente	Confirmar componentes del servicio	N/A
5.	Iniciar con el reconocimiento	Especialista de Ciberinteligencia	Se realizan actividades de reconocimiento de los activos bajo alcance como servicios, tipos de tecnología, entre otros	N/A
6.	Generar el descubrimiento	Especialista de Ciberinteligencia	Se identifica el mapeo de activos	N/A
7.	Realizar la enumeración	Especialista de Ciberinteligencia	Se identifica la identificación puntual de puertos, servicios, identificación de superficie de ataque y funcionamiento de cada activo bajo alcance	N/A
8.	Análisis de vulnerabilidades	Especialista de Ciberinteligencia	Se realiza el análisis de vulnerabilidades mediante 3 principales actividades: análisis manual, análisis automatizado y búsqueda en fuentes conocidas	N/A
9.	Revisar si se requiere presentación de avance	Especialista de Ciberinteligencia	Revisar si se requiere realizar la presentación para reportar el avance del servicio contratado. ¿se requiere presentación? Si: Continuar con la actividad 10. No: Continuar con la actividad 11.	

10.	Presentar avance	Especialista de Ciberinteligencia	Se presentan las actividades realizadas, así como los activos y vulnerabilidades identificadas en cada uno de ellos. De igual manera se proponen las diferentes vulnerabilidades a explotar (realizar validación de las mismas o descartar falsos positivos) para definir ventanas de tiempo	Reunión de avance
11.	Evaluar si se requiere la explotación de vulnerabilidades	Especialista de Ciberinteligencia	Evaluar si se requiere la explotación de vulnerabilidades. ¿Se requiere explotar vulnerabilidades? Si: Continuar con la actividad 12. No: Continuar con la 14	
12.	Explotar	Especialista de Ciberinteligencia	Se realiza la validación de vulnerabilidades, así como la preparación de actividades post-explotación	N/A
13.	Post-explotar	Especialista de Ciberinteligencia	Se realizan actividades de Post-explotación de acuerdo con el alcance de la fase	N/A
14.	Revisar si se requiere generar una presentación ejecutiva	Especialista de Ciberinteligencia	Revisar si se requiere generar una presentación ejecutiva para el servicio contratado. ¿se requiere presentación ejecutiva? Si: Continuar con la actividad 15. No: Continuar con la actividad 16	N/A
15.	Generar presentación ejecutiva	Especialista de Ciberinteligencia	Se regenera la documentación relacionada	Presentación ejecutiva final
16.	Generar entregables	Especialista de Ciberinteligencia	Se regenera la documentación relacionada	Documentos técnicos
17.	Revisar los entregables	Entrega de Servicios	Revisar los entregables ¿Existen comentarios en la documentación? Si: Generar comentarios para su corrección (ir al paso 18). No: Validar los entregables para su entrega al Cliente (ir al paso 19).	Documentos técnicos
18.	Realizar ajustes en los entregables	Líder de ciberinteligencia	Realizar ajustes en los entregables y enviar nuevamente	Documentos técnicos

			a Entrega de Servicios para su validación (regresar al paso 17).	
19.	Recibir entregables y firmar de conformidad	Cliente	Recibir entregables y firmar de conformidad. Fin del procedimiento.	Documentos técnicos
Fin del procedimiento				

6. Documentos relacionados

•PR-ENS-001 Gestión de Proyectos.

7. Anexos

N/A