



Grupo Empresarial
Datasoft

AVI-2023-PLAN DE TRABAJO
ANÁLISIS DE VULNERABILDADES INS

Instituto Nacional de Seguros

Desarrollado por:
Servicios de Consultoría Datasoft

13 de abril 2023

VERSION 2.0

IDENTIFICACIÓN DE DOCUMENTO

DATOS DEL DOCUMENTO

Nombre de archivo	AVI-2021- Plan de Trabajo Análisis de Vulnerabilidades INS
Fecha de Creación	13 de abril 2023
Última modificación	20 de abril 2023

HISTORIA DE REVISIÓN DEL DOCUMENTO

Fecha	Versión	Actualizado por	Información de los cambios
13/04/2023	1.0	Datasoft	Primera versión
19/05/2023	2.0	Datasoft	Segunda versión

INTRODUCCIÓN

El presente documento constituye el entregable “AVI-2021- Plan de Trabajo Análisis de Vulnerabilidades INS”, cuyo resultado será utilizado para integrar el nivel global de vulnerabilidad (efectividad y madurez de la seguridad de la información) para un cálculo de riesgo dentro de la realidad institucional; así como las acciones específicas que deben seguirse para su solución en los diferentes componentes que conforman la plataforma tecnológica del Instituto Nacional de Seguros (INS).

La identificación detallada de las vulnerabilidades técnicas en la infraestructura tecnológica del Instituto Nacional de Seguros forma parte del nivel global de vulnerabilidad en que se realiza la gestión de TI y seguridad de la información; y así mismo que tiene una incidencia en el nivel de riesgo total de la institución, puesto que denota el nivel de exposición en el que se encuentran estos activos de información aunado a la efectividad de los controles generales de TI.

La relación entre vulnerabilidad técnica y efectividad de controles debe potencializarse para que el Instituto Nacional de Seguros pueda establecer los elementos resolutivos necesarios para remediar estas deficiencias técnicas y evitar que se presenten nuevamente en el transcurso del tiempo, estandarizando la operación de TI con base en los requerimientos de las áreas usuarias y la misión organizacional.

Como parte servicio, se utilizarán herramientas para la identificación de vulnerabilidades de la infraestructura de red y las diferentes plataformas que soportan los procesos del Instituto Nacional de Seguros.

Una vez identificado las vulnerabilidades, se ejecutará un análisis posterior con el fin de evidenciar las brechas de seguridad existentes a través de pruebas de intrusión y explotación en un ambiente controlado (no invasivo), por lo que no afectará las operaciones y servicios que brinda el Instituto Nacional de Seguros.

El contenido de este documento asume algunos conocimientos básicos de seguridad por lo que tiene un enfoque técnico.

OBJETIVOS Y ALCANCE

OBJETIVO

Identificar y evidenciar las vulnerabilidades existentes en la plataforma tecnológica del Instituto Nacional de Seguros haciendo uso de diversas herramientas tecnológicas, según el requerimiento #R-000747

ALCANCE

El análisis de vulnerabilidades de Red Interna se llevará a cabo mediante la revisión de aquellos equipos seleccionados por el Instituto Nacional de Seguros en el direccionamiento IP que conforman la red interna, en el cual de ser posible se evidenciará la explotación de las vulnerabilidades encontradas y en caso contrario se justificará las razones por las cuáles no se expuso la vulnerabilidad.

Es importante mencionar que la ejecución de estas herramientas no afectará el desempeño tanto de la red ni de los sistemas operativos, con lo cual se asegura que dichas pruebas no interfieren con la operación y los servicios del Instituto Nacional de Seguros.

El análisis se ejecutará bajo la modalidad de pruebas de caja blanca o White box, en el cual los auditores solicitarán al Instituto Nacional de Seguros la información necesaria para la ejecución de las pruebas de forma minuciosa, incluyendo archivos de configuración y documentación necesaria.

De acuerdo con el requerimiento R-000257 el Análisis de Vulnerabilidades para la Red Interna constará de dos fases, por lo que en esta primera ejecución se estará evaluando los siguientes sitios internos del Instituto Nacional de Seguros (INS):

SITIOS RED INTERNA
Centro de Datos Principal
Centro de Datos Alterno
Dispositivos de Redes
Nube

Tabla 1: Alcance.

REQUERIMIENTOS PREVIOS

Las pruebas de Caja Blanca (White Box) sobre análisis de vulnerabilidades de red interna son pruebas ejecutadas por auditores de seguridad y pentester para evaluar un sistema interno e identificar sus debilidades. De acuerdo con el tipo análisis en el cual se debe conocer información necesaria para la ejecución de las pruebas es importante tener los requerimientos previos para que el cumplimiento de los objetivos, por lo que a continuación, se detallan los requerimientos mínimos:

1. DOCUMENTACIÓN INTERNA:

Se requiere contar con la siguiente información con el fin de definir un cronograma más exacto y asignar los recursos necesarios:

- Ubicación exacta de los sitios a evaluar.
- Horario de Ejecución.
- Rango de Direccionamiento IP para cada Sitio.
- Cantidad de Host a escanear.
- Sistemas Operativos Involucrados.
- Documentación Interna (Topologías de Red, Diagramas, Arquitecturas, Servidores, Dispositivos de Seguridad Perimetral o inventarios de Equipo).

2. APROVISIONAMIENTO DE SERVIDOR JUMP SERVER

Se requiere contar con un servidor de salto (Jump Server) que tenga comunicación con la red interna del Instituto Nacional de Seguros (INS), dicho servidor tendrá la función de almacenar las herramientas y ejecutar los escaneos de forma remota a los diferentes hosts durante la jornada laboral y fuera de ella de ser el caso.

A continuación, se muestra los requerimientos mínimos específicos de este servidor:

- **Sistema Operativo:** Windows 10 o Windows Server 2016 (o posterior con capacidad de Virtualización).
- **Memoria RAM:** mínimo 16 GB
- **Procesador:** Mínimo 4 Núcleos
- **Disco de Almacenamiento:** Mínimo 250 GB
- **Comunicación:** Deberá tener comunicación con toda la red interna del INS.
- **Internet:** Deberá tener salida a Internet.
- **Conexión:** Usuario de VPN y administrador del equipo deberán tener permisos administrativos.

En dicho servidor, se deberá instalar una máquina virtual con el Sistema Operativo Kali Linux, a través del siguiente enlace podrá obtener el .iso para la instalación: <https://www.kali.org/get-kali/#kali-live>, además deberá tener las características de **Comunicación e Internet** mencionadas anteriormente.

METODOLOGÍA

Este análisis de vulnerabilidades estará basado en los conceptos técnicos y metodología del Etical Hacker y PTES así mismo, estándares internacionales como mejores prácticas en la industria en cuanto a la gestión y resguardo de la seguridad de la información tales como: ISO-27000, ISO-27001.

El Análisis de Vulnerabilidades se realizará sobre la Red Interna del Instituto Nacional de Seguros, es decir, sistemas de información entorno a la red interna o red local del cliente sobre aquellos equipos de la organización que están expuestos a vulnerabilidades o riesgos de seguridad. Algunos ejemplos de los equipos objetivo de este ejercicio son: dispositivos de red, dispositivos de seguridad perimetral, servidores, equipos clientes, entre otros.

Cuando se habla de Análisis de Vulnerabilidades de Red Interna, se refiere a la acción de efectuar pruebas de vulnerabilidades de manera controlada y autorizada sobre sistemas de información entorno a la red interna o red local; el consultor deberá ejecutar un escaneo de la red con el fin de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, siempre tomando en cuenta se debe realizar en un ambiente supervisado en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización.

ELEMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es un estado de bienestar de la información y la infraestructura, en el que la posibilidad de robo, alteración, actualización de los servicios y la información es baja o tolerable. La gestión de la información se establece gracias a los tres pilares fundamentales de la seguridad de la información que son la confidencialidad, integridad y autenticidad, mismos que se describen en la siguiente imagen:

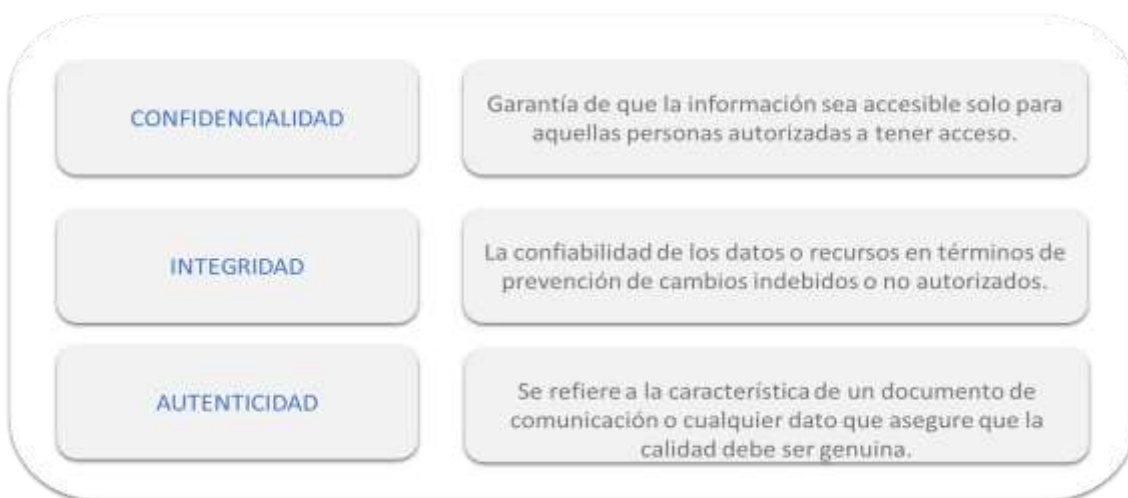


Imagen01: Elementos de Seguridad de la Información.

FASES DE ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades de red interna y las pruebas de intrusión están compuestos por un orden lógico de pasos que se deben cumplir para llevar a cabo el éxito de las pruebas.

A continuación, se detallan las fases que resumen la metodología de trabajo a utilizar:

1. Escaneo Red y Enumeración.
2. Identificación de Vulnerabilidades.
3. Explotación de las Vulnerabilidades (Pruebas de Intrusión).
4. Demostración de las Vulnerabilidades

Usualmente dichas fases se representan como un ciclo al que se denomina comúnmente círculo del hacking que se muestra a continuación.

CÍRCULO DEL HACKING

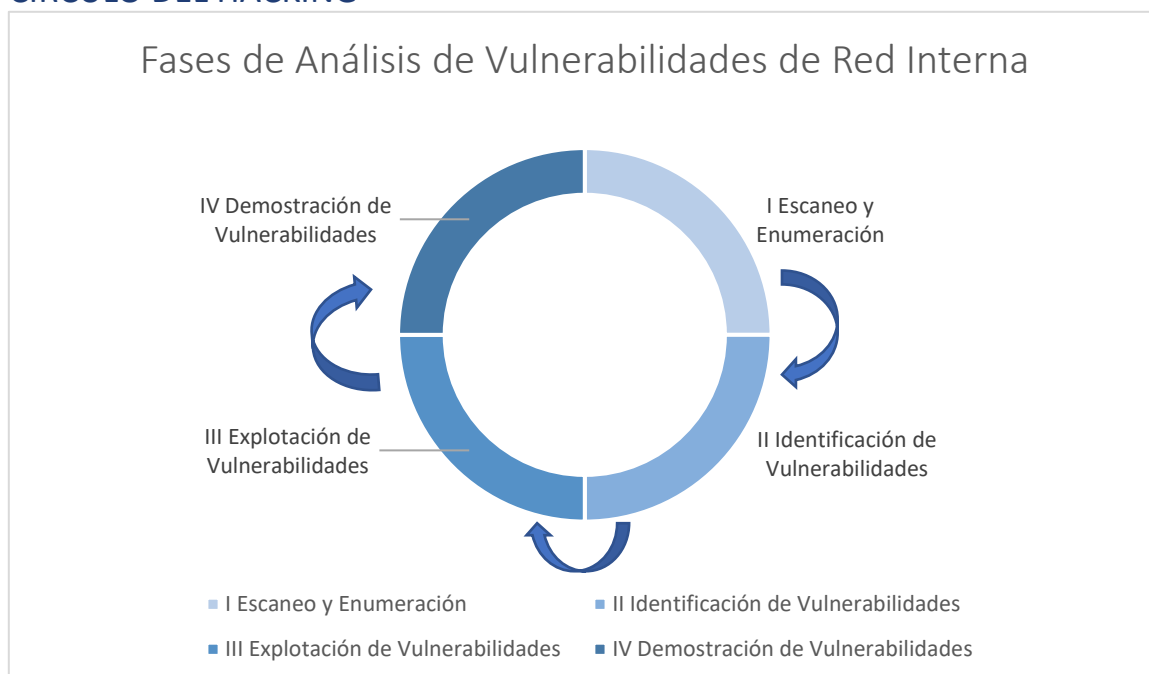


Imagen02: Círculo del hacking

A continuación, se detallan cada una de las fases que se estarán ejecutando en el análisis.

I. ESCANEEO Y ENUMERACIÓN

Durante esta fase se pretende analizar la red para identificar puertos y servicios que corresponden a los dispositivos solicitados. Además, se pretende descubrir máquinas activas en una red e identificar el tipo de sistema operativo que se ejecuta en los hosts de destino.

Esta fase permitirá crear un perfil de la organización objetivo. En este proceso, el equipo de trabajo intentará recopilar información, incluidas las direcciones IP específicas a las que se puede acceder a través de la red, el sistema operativo de los objetivos, la arquitectura del sistema y los puertos junto con sus respectivos servicios que se ejecutan en cada dispositivo.

Una vez finalizado el escaneo, el objetivo de enumerar es identificar los nombres de los equipos, usuarios, y recursos compartidos entre otra información.

Además, el propósito del escaneo es descubrir canales de comunicación explotables, sondear a tantos oyentes como sea posible y rastrear aquellos que responden o son útiles para las necesidades particulares de un atacante.

OBJETIVOS DEL PROCESO ESCANEEO Y ENUMERACIÓN

A continuación, se detalla un listado de resultados que se logran obtener en esta fase:

- Descubrir los hosts en vivo de la red, las direcciones IP y los puertos abiertos de los hosts en vivo. Usando los puertos abiertos, el auditor determinará la mejor forma de ingresar al sistema.
- Descubrir el Sistema Operativo y la arquitectura del sistema del sistema de destino. Hacerlo le da al auditor una indicación de las vulnerabilidades (basadas en el servicio) que pueden explotarse para obtener acceso al sistema de destino.
- Identificar aplicaciones específicas de versiones de un servicio en particular.
- Identificar vulnerabilidades en cualquiera de los sistemas de red. Esto ayuda a un atacante a comprometer el sistema o la red de destino a través de varios Exploit.

LISTADO DE HERRAMIENTAS DE ESCANEO DE RED

A continuación, se detalla un listado de las posibles herramientas que se utilizarán para la fase II de Escaneo de Red:




FOOTPRINTING			
N°	NOMBRE	LOGO	DESCRIPCIÓN
1	NMAP		Nmap Terminal es una potente herramienta para descubrir información sobre máquinas en una red o Internet. Le permite sondear una máquina con paquetes para detectar todo, desde servicios en ejecución y puertos abiertos hasta el sistema operativo y las versiones de software.
2	ZENMAP		Zenmap es la GUI oficial de Nmap Security Scanner. Es una aplicación multiplataforma de código abierto que tiene como objetivo hacer Nmap. Realiza un escaneo de red e internet para identificar servicios en ejecución y puertos abiertos.
3	WireShark		Wireshark es el analizador de protocolos de red más importante y ampliamente utilizado del mundo. Wireshark tiene un conjunto de características enriquecido que incluye lo siguiente: Inspección profunda de cientos de protocolos, captura en vivo y análisis fuera de línea, navegadores de paquetes estándar, datos de red, etc.

Tabla 3: Escaneo de red.

II. EVALUACIÓN DE VULNERABILIDADES

Durante esta etapa se evaluará la capacidad de un sistema o aplicación, incluidos los procedimientos y controles de seguridad actuales para resistir la explotación. Durante esta evaluación se escanea las redes en busca de debilidades de seguridad conocidas y se reconoce, mide y clasifica, cuantifica y clasifica las posibles vulnerabilidades a las amenazas en un sistema.

OBJETIVOS DEL PROCESO EVALUACIÓN DE VULNERABILIDADES

A continuación, se detalla un listado de resultados esperados de esta fase:

- Obtener la versión del sistema operativo que se ejecuta en la computadora o los dispositivos.
- Obtener los puertos IP y Protocolo de control de transmisión (TCP) / Protocolo de datagramas de usuario (UDP) que están escuchando.
- Adquirir las aplicaciones instaladas en dispositivos.
- Cuentas con contraseñas débiles
- Conseguir los archivos y carpetas con permisos débiles
- Determinar los servicios y aplicaciones predeterminados que podrían tener que desinstalarse
- Identificar el error en la configuración de seguridad de aplicaciones comunes
- Adquirir las sesiones expuestas a vulnerabilidades conocidas o notificadas públicamente
- Obtener información del software EOL / EOS
- Identificar la falta parches y revisión
- Obtener las configuraciones de red débiles y puertos mal configurados o de riesgo.

LISTADO DE HERRAMIENTAS DE EVALUACIÓN DE VULNERABILIDADES

A continuación, se detalla un listado de las posibles herramientas que se utilizarán para la fase III de Evaluación de Vulnerabilidades:

FOOTPRINTING			
N°	NOMBRE	LOGO	DESCRIPCIÓN
1	Técnicas Manuales de Identificación de Vulnerabilidades		Las técnicas manuales son inspecciones que se realizan con el objetivo de identificar vulnerabilidades en los dispositivos auditados a través del análisis de la documentación de vulnerabilidades que afectan los sistemas operativos y servicios identificados.
3	BurpSuite		Burp Suite es una plataforma integrada para realizar pruebas de seguridad de aplicaciones web. Sus diversas herramientas funcionan perfectamente juntas para soportar todo el proceso de prueba, desde la asignación inicial, hasta la búsqueda y explotación de vulnerabilidades de seguridad.
4	Nessus		Nessus es el escáner de vulnerabilidades más usado en el mundo. Previene eficientemente los ataques de red identificando las debilidades y errores de configuración que pueden ser usados para los ataques.
5	OpenVas		OpenVAS es un marco de varios servicios y herramientas que ofrece una solución integral y potente de análisis de vulnerabilidades y gestión de vulnerabilidades

Tabla 4: Herramientas de Evaluación de Vulnerabilidades

III. EXPLOTACIÓN DE VULNERABILIDADES

Esta fase pretende explotar las vulnerabilidades identificadas en la fase de evaluación con el fin de obtener acceso a los sistemas informáticos del Instituto Nacional de Seguros y así mismo, evidenciar a través de pruebas de intrusión que los dispositivos realmente son vulnerables ante ese tipo de brechas de seguridad.

Se utilizará técnicas de pruebas de Pentesting, también conocido como pruebas de pluma, el cual se define como un ataque cibernético simulado contra su sistema informático para comprobar si existen vulnerabilidades explotables. En el contexto de la seguridad, estas pruebas pueden implicar el intento de infracción de cualquier número de sistemas de aplicaciones (por ejemplo, interfaces de protocolo de aplicación (API), servidores front-end/back-end) para descubrir vulnerabilidades, como entradas no deseadas que son susceptibles a ataques de inyección de código.

Este tipo de actividades se realizarán bajo un ambiente controlado, el cual no deberá representar afectaciones en los servicios del Instituto Nacional de Seguros.

OBJETIVOS DE LA EXPLOTACIÓN DE VULNERABILIDADES

A continuación, se detalla un listado de resultados que se espera obtener de esta fase:

- Obtener el estado de la seguridad de la organización y del sistema objetivo en un momento determinado.
- Tener un perfil de la infraestructura de seguridad desde el punto de vista de un atacante.
- Comprobar el verdadero impacto de las vulnerabilidades en diferentes entornos y que criticidad puede tener para el negocio.
- Comprobar si toda la infraestructura de seguridad puede soportar ataques informáticos personalizados para la empresa.

LISTADO DE HERRAMIENTAS DE EXPLOTACIÓN DE VULNERABILIDADES

Este listado de actividades, técnicas y herramientas para la explotación de vulnerabilidades se definirán una vez se cuenten con los resultados obtenidos en las fases anteriores (Escaneo de Red y Enumeración y Evaluación de vulnerabilidades).

IV. DEMOSTRACIÓN DE VULNERABILIDADES

La última fase de la metodología representa la obtención de evidencia de las vulnerabilidades identificadas y pruebas de intrusión realizadas durante las fases anteriores. La demostración de vulnerabilidades representa a través de un informe ejecutivo la clasificación de vulnerabilidades identificadas y pruebas de intrusión realizadas para cada uno del host.

OBJETIVOS DE LA EXPLOTACIÓN DE VULNERABILIDADES

A continuación, se detalla un listado de resultados que se pretende obtener de esta fase:

- Informe ejecutivo del listado de vulnerabilidades encontradas y sus posibles soluciones.
- Informe ejecutivo con el listado de pruebas de explotación y técnicas utilizadas.

CRONOGRAMA

A continuación, se detalla el cronograma para la ejecución del análisis de vulnerabilidades sobre las direcciones IP Públicas solicitadas por el Instituto Nacional de Seguros.

CRONOGRAMA DE RED INS - ESTIMACIÓN DE FECHAS				
Evento Significativo	Duración estimada	Días	Inicio	Fin
Planificación				
Preparación de herramientas	8 hrs	1	24/04/2023	24/04/2023
Ejecución				
Centro de Datos Principal				
Escaneo de Red y Enumeración	22 hrs	3	25/04/2023	27/04/2023
Evaluación de Vulnerabilidades	22 hrs	3	28/04/2023	03/05/2023
Análisis de las Vulnerabilidades existentes	12 hrs	2	04/05/2023	05/05/2023
Explotación de Vulnerabilidades	24 hrs	4	08/05/2023	11/05/2023
Elaboración de Informes de Resultados	26 hrs	2	12/05/2023	24/05/2023
Centro de Datos Alterno				
Escaneo de Red y Enumeración	14 hrs	2	18/05/2023	19/05/2023
Evaluación de Vulnerabilidades	14 hrs	2	22/05/2023	23/05/2023

Análisis de las Vulnerabilidades existentes	6 hrs	1	24/05/2023	24/05/2023
Explotación de Vulnerabilidades	16 hrs	2	25/05/2023	26/05/2023
Elaboración de Informes de Resultados	17 hrs	2	29/05/2023	30/05/2023
Dispositivos de Redes				
Escaneo de Red y Enumeración	6 hrs	1	01/06/2023	01/06/2023
Evaluación de Vulnerabilidades	8 hrs	2	02/06/2023	05/06/2023
Análisis de las Vulnerabilidades existentes	6 hrs	1	05/06/2023	05/06/2023
Explotación de Vulnerabilidades	10 hrs	2	06/06/2023	07/06/2023
Elaboración de Informes de Resultados	12 hrs	1	08/06/2023	08/06/2023
Nube				
Escaneo de Red y Enumeración	20 hrs	3	12/06/2023	14/06/2023
Evaluación de Vulnerabilidades	20 hrs	3	15/06/2023	19/06/2023
Análisis de las Vulnerabilidades existentes	12 hrs	2	20/06/2023	21/06/2023
Explotación de Vulnerabilidades	24 hrs	3	22/06/2023	26/06/2023
Elaboración de Informes de Resultados	22 hrs	2	27/06/2023	28/06/2023
Total	321 hrs	44		

Tabla 5: Cronograma de Ejecución

Nota: el tiempo mostrado en la tabla anterior es un estimado y se facturará únicamente el tiempo efectivo empleado por el equipo de trabajo.

Las vulnerabilidades identificadas como críticas y que generen un alto riesgo a nivel de la organización, se estarán comunicando de inmediato a través de los diferentes medios de comunicación.

El cronograma de trabajo propuesto pretende generar informes al finalizar la evaluación de cada sitio, esto para que el INS pueda obtener resultados de manera progresiva y no tenga que esperar hasta el final del ejercicio para obtener los informes.