PLAN DE PRUEBAS DE ANÁLISIS DE VULNERABILIDADES, HACKING ÉTICO Y RETEST

DOCUMENTO CONFIDENCIAL

Elaborado por:

password

Versión 1.0

Enero, 2026 Bogotá D.C

Historial de versiones

Id	Fecha (dd/mm/aa)	Versión	Descripción	Elaborado por	Revisado por
1	23/01/2026	1.0	Plan de pruebas, Ethical Hacking y Retest	Rodrigo Diaz	Password Consulting Services S.A.S

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. DEFINICIONES 4
5. CONTENIDO 4
5.1 Metodología a Utilizar 5
5.1.1. FASE 1. Identificación de vulnerabilidades puertos y servicios. 5
5.1.2. FASE 2. Análisis técnico de vulnerabilidades 6
5.1.3. FASE 3. Análisis de vulnerabilidades asistido con Inteligencia Artificial 7
5.1.4. FASE 4. Pruebas de seguridad (Hacking Ético) 8
5.1.5. FASE 5. Generación y socialización de resultados 9
5.1.6. FASE 6. Verificación final del estado de las vulnerabilidades (Retest) 10
5.2 Tipo de Prueba y Condiciones Iniciales 11
6. CRONOGRAMA 12
6.1. RollBack: 15
7. PLAN DE COMUNICACIONES 15

1. INTRODUCCIÓN

En este documento se relacionan todas las actividades a realizar en el proyecto de seguridad para TRANSMILENIO, estos ejercicios involucran actividades de análisis de vulnerabilidades, hacking ético y retest para la cantidad de activos que se describen en el alcance, también se establece un cronograma de trabajo acorde a la cantidad de activos y se mencionan las herramientas que se usaran a lo largo del proyecto.

2. OBJETIVO

Presentar la metodología y tiempos estimados de ejecución para que este documento sea aprobado por TRANSMILENIO, una vez recibida la aprobación, se daría inicio a todas las actividades aquí descritas.

3. ALCANCE

Se han proporcionado un total de 61 activos a evaluar, las direcciones IP de esos activos se relaciona en la siguiente tabla:

Direcciones IP			
172.16.34.6	10.0.1.16	172.16.34.13	192.168.100.138
172.16.34.7	192.168.100.113	172.16.34.14	192.168.100.118
172.16.34.8	192.168.100.5	172.16.34.30	192.168.100.117
172.16.34.18	172.16.34.26	192.168.100.136	192.168.100.191
172.16.34.10	172.16.34.27	192.168.100.135	192.168.100.160
172.16.34.21	172.16.31.48	192.168.100.134	192.168.100.162
172.16.34.24	192.168.100.130	172.16.34.4	192.168.100.145
172.16.34.11	192.168.100.139	192.168.100.32	172.16.34.25
172.16.34.15	192.168.100.40	192.168.100.33	192.168.100.107
172.16.34.28	192.168.100.56	192.168.100.34	192.168.100.193
172.16.34.12	192.168.100.178	192.168.50.8	192.168.100.192
172.16.34.16	192.168.100.163	192.168.100.169	192.168.100.165
192.168.100.132	192.168.100.155	192.168.100.35	192.168.100.154
11.0.2.5	172.16.31.22	192.168.100.36	
11.0.2.9	192.168.100.125	192.168.100.159	
172.16.31.45	192.168.100.119	192.168.100.110	

Tabla 1. Activos a evaluar

4. DEFINICIONES

- **Activo de Información**: Cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse. (ISO/IEC 27001:2013).

- **Análisis**: Examen o evaluación detallada de un objeto, articulo o infraestructura para obtener una mejor comprensión de su situación actual, problema o necesidad latente.

- **Vulnerabilidad:** Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

- **Ethical Hacking:** Pruebas de seguridad que permiten poner en evidencia la presencia de vulnerabilidades sobre uno o varios activos de información.

- **Retest:** Una fase de pruebas de seguridad que implica volver a verificar las vulnerabilidades previamente identificadas después de que hayan sido corregidas o mitigadas. El objetivo es confirmar que las soluciones implementadas han eliminado eficazmente las debilidades identificadas.

5. CONTENIDO

En este numeral se revisan las herramientas a utilizar y la metodología que se aplicará a los activos de información descritos en el alcance, mencionando una a una las fases y entregables que se deben generar como resultado de cada fase:

Nota: La presente metodología consigna las actividades metodológicas para ambas pruebas, tanto las pruebas de vulnerabilidades como las pruebas de hacking ético. Lo anterior dado que las pruebas de hacking ético permiten comprobar la existencia de vulnerabilidades a través de las pruebas de hacking ético se realiza la validación de falsos positivos sobre la información entregada por las pruebas de vulnerabilidad.

Por lo anterior, las pruebas de vulnerabilidad se convierten en un insumo indispensable para planear las pruebas de hacking ético y dichas pruebas de hacking ético corroboran los resultados de las vulnerabilidades con duda que fueron identificadas en las pruebas de vulnerabilidad. Esto mantiene un vínculo entre ambas pruebas y por consiguiente la relación y e intersección en las metodologías.

A continuación, se presenta la metodología que se aplica para cubrir ambos tipos de pruebas:

5.1 Metodología a Utilizar

A continuación, se presenta la metodología OSSTMM (Open Source Security Testing Methodology Manual) y OWASP (Open Web Application Security Project), todas en su última versión, y de las cual se derivan las siguientes actividades:



Figura 1. Metodología a utilizar de pruebas de vulnerabilidad y Ethical hacking

5.1.1. FASE 1. Identificación de vulnerabilidades puertos y servicios.

Objetivo

Establecer la superficie de ataque inicial del objetivo. Esta fase se centra en el descubrimiento y enumeración de todos los activos accesibles (hosts, dominios, aplicaciones), recopilando información clave como puertos abiertos, servicios activos y las versiones de software y tecnologías expuestas. El fin es crear un mapa detallado del entorno para identificar vectores de entrada potenciales y puntos de interés para las siguientes fases.

Alcance

Se centra en el **reconocimiento activo** (escaneo de puertos, sondeo de servicios) sobre los activos definidos en el alcance del ejercicio. Incluye el uso de herramientas automatizadas para una detección inicial de vulnerabilidades conocidas (ej. CVEs en versiones de software expuestas), pero *no* incluye la explotación o validación manual de dichas vulnerabilidades.

Actividades

- **Escaneo y Enumeración de Red (Scanning):** Identificación de hosts activos, escaneo de puertos (TCP/UDP) para descubrir servicios expuestos (ej. SMB, SMTP, SSH, HTTP, RDP).

- **Fingerprinting de Servicios y Versiones:** Determinación precisa de las tecnologías, sistemas operativos, aplicaciones y versiones de software en ejecución en cada puerto abierto.

- **Escaneo Automatizado de Vulnerabilidades:** Ejecución de escáneres de vulnerabilidades (como Nmap scripts, Nessus, Nikto, etc.) para identificar configuraciones incorrectas comunes y vulnerabilidades "de fruta madura" (low-hanging fruit) basadas en las versiones detectadas.

5.1.2. FASE 2. Análisis técnico de vulnerabilidades

Objetivo

Validar, depurar y categorizar los hallazgos de la Fase 1. El objetivo principal es aplicar el criterio y la experiencia de los analistas de Password para confirmar la existencia real de las vulnerabilidades reportadas por las herramientas automatizadas, descartar los falsos positivos y realizar una evaluación inicial del riesgo de cada hallazgo confirmado. Esta fase filtra el "ruido" y enfoca los esfuerzos de las fases posteriores únicamente en amenazas verificadas.

Alcance

Esta limitado a la revisión y validación de los datos recolectados. Incluye la inspección manual, pero no intrusiva, de servicios y aplicaciones para confirmar o desmentir los hallazgos. No se realizan intentos de explotación, sino de corroboración (ej. verificar banners manualmente, probar configuraciones por defecto conocidas, comparar versiones exactas con bases de datos de exploits).

Actividades

- **Consolidación y Correlación de Hallazgos:** Agrupar y cruzar los resultados de las distintas herramientas de la Fase 1 (escáneres de puertos y de vulnerabilidades) para obtener una vista unificada de los activos y sus debilidades potenciales.

- **Verificación Manual y Descarte de Falsos Positivos:** Análisis crítico de cada vulnerabilidad reportada. Se realizan comprobaciones manuales (ej. revisión de cabeceras HTTP, conexión a servicios para verificar banners, análisis de respuestas de error) para confirmar que la vulnerabilidad es real y no un error del escáner.

- **Investigación y Contextualización de Vulnerabilidades:** Búsqueda de información pública (bases de datos de CVEs, Exploit-DB, reportes de seguridad) sobre las vulnerabilidades *confirmadas* para entender su impacto potencial, su severidad y la existencia de pruebas de concepto (PoCs) o exploits públicos.

- **Priorización Inicial de Hallazgos:** Clasificación de las vulnerabilidades validadas según su severidad (Crítica, Alta, Media, Baja) y su aparente explotabilidad, creando una lista depurada que servirá como entrada para las siguientes fases.

5.1.3. FASE 3. Análisis de vulnerabilidades asistido con Inteligencia Artificial

Objetivo

Enriquecer el análisis tradicional de vulnerabilidades (Fase 2) utilizando modelos de Inteligencia Artificial. El objetivo es identificar patrones complejos, correlacionar hallazgos aparentemente aislados y descubrir vectores de ataque no evidentes que las herramientas convencionales y el análisis manual inicial podrían pasar por alto. Esta fase busca optimizar la priorización de objetivos para la fase de Hacking Ético, enfocando los esfuerzos en las amenazas más probables y de mayor impacto.

Alcance

Aplicación de herramientas basadas en IA (como LLMs entrenados en seguridad, plataformas de análisis predictivo o correlación avanzada) sobre el conjunto de vulnerabilidades *ya validadas* en la Fase 2. Incluye el análisis de código (SAST) asistido por IA (si se dispone del código), la generación de hipótesis de cadenas de ataque (attack chains) y la evaluación contextual de la explotabilidad de un fallo.

Actividades

- **Correlación Avanzada de Hallazgos:** Utilización de IA para cruzar datos de todos los servicios y aplicaciones analizadas, identificando cómo

vulnerabilidades de bajo impacto en diferentes sistemas podrían ser encadenadas para lograr un impacto crítico.

- **Análisis Predictivo y de Lógica de Negocio:** Aplicación de modelos de IA para analizar el comportamiento de la aplicación o revisar código fuente en busca de fallos de lógica de negocio (ej. secuencias de pasos inseguras) que no se basan en firmas de CVEs conocidas (este punto aplica solo en casos específicos).

- **Generación de Pruebas de Concepto (PoC):** Asistencia de la IA para generar borradores de *scripts* o *payloads* de prueba de concepto (PoC) adaptados al entorno y tecnología específicos del objetivo, agilizando la preparación para la fase de explotación.

- **Priorización de Vectores de Ataque:** Re-evaluación de la lista de vulnerabilidades priorizadas, esta vez clasificándolas no solo por su severidad (CVSS) sino por su *probabilidad real de explotación* en el contexto del sistema evaluado, según el análisis de la IA.

5.1.4. FASE 4. Pruebas de seguridad (Hacking Ético)

Objetivo

Demostrar el impacto real y tangible de las vulnerabilidades identificadas. El objetivo de esta fase es la explotación controlada de los vectores de ataque priorizados para obtener acceso no autorizado, escalar privilegios o acceder a información sensible. A diferencia de las fases anteriores de *análisis*, esta fase se centra en la *ejecución* activa de ataques simulados para validar el riesgo.

Alcance

Se enfoca estrictamente a la explotación activa y controlada de las vulnerabilidades confirmadas. Se ejecutan pruebas de penetración siguiendo las reglas de enfrentamiento (Rules of Engagement - RoE) acordadas, con el fin de evitar interrupciones de servicio no deseadas. **El alcance incluye tanto la explotación manual como la asistida por IA** para la adaptación de *payloads* o la evasión de defensas.

Actividades

- **Explotación de Vulnerabilidades (Exploitation):** Ejecución de pruebas de concepto (PoCs) y *exploits* (públicos o modificados) contra los servicios,

aplicaciones y configuraciones vulnerables para ganar un acceso inicial (ej. Remote Code Execution, SQL Injection, Server-Side Request Forgery).

- **Post-Explotación:** Una vez obtenido un acceso, se intentan técnicas para consolidar la persistencia, escalar privilegios (vertical y horizontalmente) y realizar movimientos laterales (si el alcance lo permite) para identificar el alcance máximo del compromiso.

- **Adaptación de Cargas Útiles (Payloads) con IA:** Uso de herramientas de IA para modificar y ofuscar *payloads* de explotación, con el objetivo de evadir sistemas de detección como Antivirus (AV) o Web Application Firewalls (WAF).

- **Exfiltración de Pruebas (Data Exfiltration):** Búsqueda y extracción controlada de información sensible (como "banderas" o *flags*, archivos de configuración, extractos de bases de datos) que sirva como evidencia irrefutable del impacto del ataque.

- **Documentación Rigurosa de Evidencia:** Registro detallado paso a paso (con capturas de pantalla, comandos y *scripts* utilizados) de cada explotación exitosa, demostrando la cadena de ataque (attack chain) completa.

5.1.5. FASE 5. Generación y socialización de resultados

Objetivo

Consolidar, documentar y comunicar de manera efectiva los hallazgos obtenidos en las fases de análisis de vulnerabilidades y de hacking ético, generando una serie de documentos que den una visibilidad del estado actual de la infraestructura evaluada incluyendo el riesgo de explotación que se evidencie en la fase de hacking ético.

Estos documentos presentados luego de la fase de hacking ético permiten que TRANSMILENIO comprenda tanto el inventario de debilidades como el riesgo real demostrado.

Alcance

Elaborar una serie de entregables que permitan a TRANSMILENIO tener una visibilidad tanto gerencial como técnica de todos los hallazgos o vulnerabilidades identificadas durante el procedimiento, los entregables son:

- Informe ejecutivo con información clara de todo el proceso.

- Informe ejecutivo con el detalle técnico de vulnerabilidades y remediación.
- Presentación diapositiva para socialización.
- Plan de explotación actualizado con el estado final de las pruebas propuestas.

Actividades

Esta fase presenta los resultados tanto de la fase de análisis de vulnerabilidades como de las pruebas de seguridad:

- **Generación de resultados de análisis de Vulnerabilidades:** Creación de un informe técnico y ejecutivo que detalla todas las vulnerabilidades identificadas y validadas, priorizadas por riesgo (CVSS y contexto de IA), y se descartan los falsos positivos.

- **Documentación de Explotación:** Redacción del informe técnico final y otro ejecutivo, que contienen los resultados de la fase de análisis de vulnerabilidades y se enfoca en la metodología de explotación (PoC), las cadenas de ataque utilizadas, la evidencia (capturas de pantalla, datos exfiltrados) y el impacto demostrado.

- **Elaboración de Resumen Ejecutivo:** Creación de un resumen de alto nivel (para la gerencia) que explica en términos de negocio los riesgos críticos *demostrados* y su impacto.

- **Presentación Final de Resultados:** Sesión de socialización formal con todos los *stakeholders* (técnicos y gerenciales) para presentar los resultados finales, demostrar las explotaciones más críticas y entregar las recomendaciones de remediación definitivas.

5.1.6. FASE 6. Verificación final del estado de las vulnerabilidades (Retest)

Objetivo

Validar y verificar la efectividad de las acciones de remediación implementadas por TRANSMILENIO. El objetivo principal es confirmar que las vulnerabilidades reportadas en la Fase 5 han sido corregidas, mitigadas o gestionadas adecuadamente, asegurando que los vectores de ataque (demostrados en la Fase 4) ya no son viables y que el riesgo ha sido reducido a un nivel aceptable.

Alcance

Está estrictamente limitado a la Re-evaluación de los hallazgos documentados en el informe final. No constituye una nueva prueba de penetración completa, sino una auditoría de validación enfocada. Las pruebas se dirigen únicamente a los sistemas, parámetros y vectores previamente identificados como vulnerables para confirmar su estado de remediación.

Actividades

- **Planificación del Retest:** TRANSMILENIO informa a Password que han ejecutado satisfactoriamente todo el proceso de remediación y están listos para ejecutar nuevamente esta fase de escaneos automatizados con los respectivos análisis manuales y asistidos por IA.

- **Ejecución de Pruebas de Verificación:** Re-ejecución metódica de las Pruebas de Concepto (PoC) y cadenas de ataque (attack chains) que fueron exitosas en la Fase 4, con el fin de confirmar si la explotación sigue siendo posible.

- **Análisis del Estado de Remediación:** Evaluación de los resultados de las pruebas para determinar si cada vulnerabilidad está:
    - **Corregida:** La vulnerabilidad ha sido erradicada desde la raíz.
    - **Mitigada:** La vulnerabilidad de raíz puede persistir, pero un control compensatorio (como un WAF) ahora bloquea efectivamente su explotación.
    - **No Corregida:** La vulnerabilidad sigue siendo explotable.

- **Generación de Informe de Retest:** Creación de un informe de seguimiento (Versión 2 del informe técnico) que actualiza el estado de cada vulnerabilidad reportada (Persistente, Remediada o Nueva en el caso de que se introduzcan nuevas vulnerabilidades).

5.2 Tipo de Prueba y Condiciones Iniciales

Se ha establecido realizar el procedimiento de manera presencial con las condiciones que se relacionan a continuación:

a. Pruebas a la infraestructura y aplicaciones internas (no expuestas a internet).

- **Tipo de prueba: "Caja Gris"**. Las pruebas se realizarán en una sede de TRANSMILENIO. Se simula a un atacante que ha logrado obtener un punto de apoyo en la red interna (ej. un dispositivo de empleado comprometido, un atacante en la LAN).
- **Objetivos:** TRANSMILENIO proporcionará el listado de objetivos (URLs, rangos IP) accesibles desde el punto de acceso inalámbrico o cableado que se designe.
- **Condiciones:** Todos los controles de seguridad internos habilitados.

6. CRONOGRAMA

#	Fecha	Hora de inicio	Hora de fin	Actividades a realizar	Resultados esperados	Genera indisponibilidad
1	23/01/26	8:00	18:00	**Planeación preliminar y programación de actividades** Elaboración del plan de pruebas, presentación y aceptación del plan con base en los activos proporcionados por el TRANSMILENIO.	Plan de pruebas con descripción de actividades a realizar con previa aprobación.	NO
2	28/01/26	8:00	16:00	**Descubrimiento de servicios internos y externos** Realizar el descubrimiento de puertos y servicios que tienen los objetivos en la red. Identificación de sistemas operativos, versiones de servicios web y banners mediante herramientas manuales y automatizadas.	Identificación de servicios y puertos que tiene abiertos/expuestos las direcciones IP Externas.	NO
3	28/01/26	16:00	17:00	**Verificación de servicios y operatividad** Se valida que los servicios de la infraestructura tecnológica analizada,	Los servicios deben quedar operativos y sin causar ninguna afectación	NO

#	Fecha	Hora de inicio	Hora de fin	Actividades a realizar	Resultados esperados	Genera indisponibilidad
				presenten normalidad operativa.		
4	29/01/26 al 30/01/26	08:00	18:00	**Análisis de vulnerabilidades regular y asistido por IA** Revisión de las detecciones bajo criterio humano experto y asistido por inteligencia artificial para clasificar y priorizar las de mayor severidad.	Establecer la superficie de ataque real que presentan los activos evaluados de acuerdo con las detecciones analizadas.	NO
5	02/02/26	8:00	9:00	**Elaboración del plan de explotación (Hacking Ético)** Se genera el plan de pruebas de seguridad o hacking ético y se envía al equipo de TRANSMILENIO para su aprobación y posterior ejecución.	☑ Presentar los hallazgos y las prioridades a tener en cuenta en el plan de remediación o mitigación. ☑Obtener aprobación del plan de explotación (Plan de Hacking Ético) por escrito para ejecutar las pruebas.	NO
6	04/02/26 al 11/02/26	8:00	18:00	**Ejecución del plan de pruebas de seguridad (Hacking Ético)** Ejecutar las pruebas propuestas en el plan de pruebas (Explotación) con base en la experiencia de Password y con apoyo de inteligencia artificial para los casos que requieran sofisticación.	Ejecutar las pruebas propuestas dentro del plan de pruebas que se encuentren autorizados por TRANSMILENIO.	Algunas pruebas podrían generar indisponibilidad, el horario de ejecución depende de lo que apruebe TRANSMILENIO.
7	12/02/26 al 16/02/26	8:00	18:00	**Elaboración de informes Post-Explotación** Documentar toda la evidencia recolectada durante la fase de pruebas	Entregables de la fase de Hacking Ético y socialización con TRANSMILENIO para dar a conocer	NO

#	Fecha	Hora de inicio	Hora de fin	Actividades a realizar	Resultados esperados	Genera indisponibilidad
				(Explotación) en informe ejecutivo y una presentación para socializar con TRANSMILENIO.	ciber riesgos de acuerdo con los hallazgos.	
8	19/02/26	15:00	18:00	**Socialización de resultados** Presentar los resultados más relevantes obtenidos de la fase de pruebas (Explotación).	Dar a conocer a TRANSMILENIO la superficie de ataque que puedan tener los activos evaluados y dar las recomendaciones que apliquen en cada caso.	NO
9	23/02/26	18:00	05:00 Día siguiente	**Retest** Ejecución del análisis de vulnerabilidades después que la entidad ha aplicado las remediaciones. **Tiempo de espera para remediación: 4 Semanas (Entrega de Váucher de ejecución)**	Verificación de la efectividad de las remediaciones o medidas compensatorias temporales que se hayan aplicado en los activos vulnerables.	NO

Tabla 2. Cronograma de actividades

6.1. RollBack:

Solo aplicarán si fallan los resultados de las actividades de acuerdo al cronograma propuesto:

#	Actividad del cronograma que falla	Incidente observado o reportado	Acciones a realizar	Resultados esperados
1	2	En caso de que las pruebas de reconocimiento fallen, las pruebas se inician nuevamente.	Determinar las versiones de los servicios que se encuentran publicados. Identificar las vulnerabilidades que tienen actualmente las direcciones públicas.	Detección de vulnerabilidades, servicios vulnerables, CVEs asociados y Exploits públicos.
2	6	En caso de que se reporte afectación de servicio, se detienen las pruebas.	No se generan más peticiones a los equipos evaluados.	Los servicios vuelven a la normalidad.

Tabla 3. Actividades RollBack

7. PLAN DE COMUNICACIONES

Nombre	Cargo	Empresa	Correo	Celular	Información a Comunicar	Medio de Comunicación
Julián Rey	Supervisor del contrato	Transmilenio S. A	julian.rey@transmilenio.gov.co	300 2022914	Inicio y terminación de las pruebas	Correo electrónico Llamada Telefónica
Rodrigo Diaz	Consultor	Password Consulting Services	rodrigo.diaz@password.com.co	314 5040093	Inicio y terminación de las pruebas	Correo electrónico Llamada Telefónica
Jackeline Diaz	Coordinadora de Proyectos	Password Consulting Services	jackeline.diaz@password.com.co	310 7539051	Inicio y terminación de las pruebas	Correo electrónico Llamada Telefónica

Tabla 4. Plan de comunicaciones