INFORME DE ANÁLISIS DE VULNERABILIDADES

GOBERNACIÓN
VALLE DEL CAUCA

Documento Confidencial
Elaborado por:

Versión 1.0

DICIEMBRE 2021
Bogotá D.C.

CONTENIDO

1. OBJETIVO

El objetivo de este documento es presentar de forma ejecutiva el resultado de las Pruebas de Vulnerabilidad, realizadas a la Infraestructura interna de la **GOBERNACIÓN DEL VALLE DEL CAUCA**, incluyendo: la descripción de las pruebas realizadas, los elementos evaluados y las vulnerabilidades identificadas junto con su nivel de criticidad como línea base y de seguimiento, así como las conclusiones y plan de remediación.

Adicionalmente, como parte de los entregables, se libera un informe de tipo técnico, el cual contiene el detalle de los hallazgos y procedimientos técnicos para corregir las vulnerabilidades identificadas.

2. ALCANCE

Las pruebas realizadas tuvieron como alcance la **Red Interna** de acuerdo con el listado de equipos entregados por la **GOBERNACIÓN DEL VALLE DEL CAUCA**. El detalle de los equipos evaluados se presenta en la sección.

3. EQUIPOS EVALUADOS

A continuación, se presenta el listado de objetivos evaluados durante la ejecución de las pruebas, los cuales fueron proporcionados por la Entidad**.**

a. **Red Interna: 24 IP's Interna:** Direcciones IP de la red internas:

SE ELIMINA POR SER INFORMACIÓN CLASIFICADA

Se identifican 20 vulnerabilidades **EXTREMAS** sobre la infraestructura interna de la **GOBERNACIÓN DEL VALLE DEL CAUCA** las cuales necesitan inmediatamente tratamiento por parte de los encargados de las soluciones.

4. TIPO DE PRUEBA Y CONDICIONES INICIALES

Las pruebas de vulnerabilidad realizadas fueron de tipo “Caja Gris”. Así mismo, la condiciones en las que se llevaron a cabo las pruebas se establecieron de tal forma que permitieran identificar las debilidades en cada uno de los equipos (IPs) objetivo contando con todos los controles de seguridad que la Entidad tiene actualmente. Su distribución y condiciones fueron las siguientes:

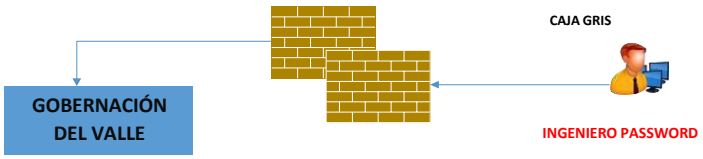
Notas: Se aclara que las vulnerabilidades detectadas dentro de la red interna fueron identificadas con los controles de seguridad con los que cuenta actualmente la Entidad. Lo anterior, dado que se desea conocer el nivel real de vulnerabilidad y debilidad de cada equipo que se encuentra de la red. Es decir, simulando un escenario en el cual un atacante informático obtenga acceso a la red bajo dichas condiciones.

5. ESCENARIO DE PRUEBAS

El escenario empleado para las pruebas de seguridad es el siguiente:

a. Pruebas Internas dentro de la red de usuarios de la **GOBERNACIÓN DEL VALLE DEL CAUCA**. En estas pruebas se llevó a cabo la evaluación de las Direcciones IP que son accesibles desde la red interna. La prueba se llevó a cabo usando una conexión directa del equipo de pruebas en la red interna de la Entidad.

Estos puntos se pueden identificar a continuación:



Gráfica 1. Escenario de las pruebas

6. FASES PARA LA EJECUCIÓN DE LAS PRUEBAS - METODOLOGÍA

Como metodología base para la identificación de vulnerabilidades se utilizó el marco de referencia **OSSTMM** (Open Source Security Testing Methodolgy Manual) y

OWASP (Open Web Application Security Project), todas en su última versión, de las cuales se derivan las siguientes actividades:

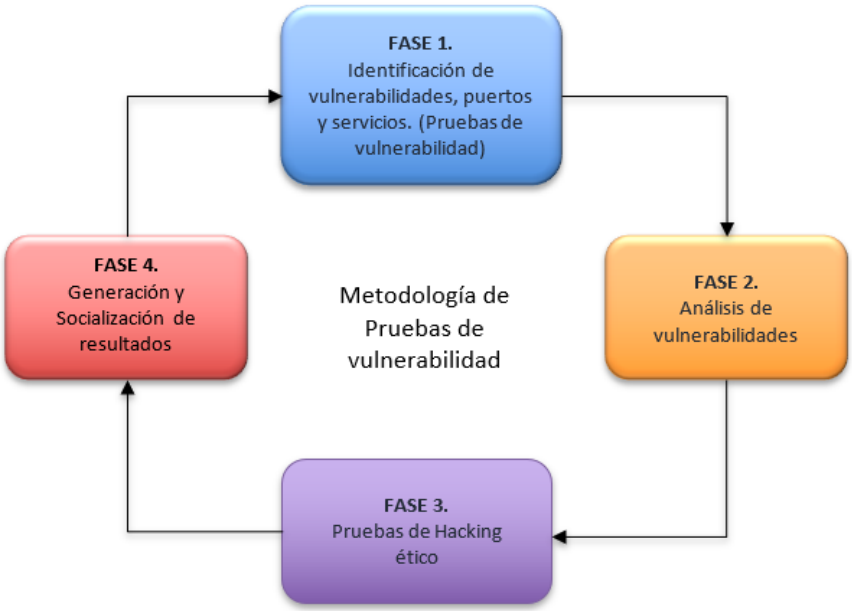


Figura 1. Metodología – Pruebas de Vulnerabilidad

CVE (Common Vulnerabilities and Exposures)

El CVE (Common Vulnerabilities and Exposures) es la lista de vulnerabilidades de seguridad de la información públicamente conocidas. Para llevar un control de esta lista a cada vulnerabilidad que se identifica se le asigna un código de identificación único conocido como identificador CVE (CVE-ID). Este identificador está formado por las siglas ID seguidas por el año en que es registrada la vulnerabilidad y un número consecutivo de cuatro dígitos. Para las pruebas efectuadas en la entidad se identificó con las herramientas automáticas el código CVE para todas las vulnerabilidades a las que aplica. Por lo tanto, en el informe técnico que se entrega como parte de este informe, se cuenta con la asignación del número de CVE a cada una de las vulnerabilidades según aplique.

OWASP (Open Web Application Security Project)

Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación,

herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

Fases para la Ejecución de las Pruebas

A continuación, se describe cada una de las fases de la metodología:

FASE 1. Identificación de vulnerabilidades puertos y servicios. (Pruebas de vulnerabilidad)

Alcance

Esta fase tiene como alcance, la identificación de vulnerabilidades **(Reconocimiento, escaneo e identificación de Servicios)** de los dispositivos de INDUMIL presentados en el numeral 3. Equipos evaluados.

Objetivo

Esta fase contempla las actividades relacionadas con el descubrimiento de los dispositivos evaluados. Así mismo, permite obtener información significativa del estado actual de cada uno de los equipos, por ejemplo: la versión del sistema operativo, los servicios que tiene abiertos hacia otros equipos y las versiones de dichos servicios. Este último, permite determinar si el servicio es vulnerable y si existen alternativas para explotar dicha debilidad en el equipo.

FASE 2. Análisis de vulnerabilidades

Alcance

Esta fase tiene como alcance, el **Análisis de resultados inicial y la construcción del plan de explotación** sobre las vulnerabilidades identificadas en la Fase 1.

Objetivo

La construcción del plan de explotación se lleva a cabo una vez se identifican las vulnerabilidades que requieren comprobarse mediante técnicas más avanzadas, algunas de ellas, que podrían llegar a generar afectación de servicio. Sin embargo, cada una de las pruebas que se documenta dentro del plan de explotación, es previamente evaluada, con el fin de determinar si la prueba genera degradación o afectación parcial/total de los servicios.

FASE 3. Pruebas de Hacking Ético (NO REALIZADA)

Alcance

Esta fase contempla la ejecución de las pruebas alternativas de verificación de vulnerabilidades y ataques de hacking ético. Por lo tanto, son ejecutadas en los horarios acordados con la entidad, y dentro del cual se ejecutan los ataques de forma monitoreada y controlada. Lo anterior, con el fin de prevenir cualquier falla o afectación en las operaciones normales de los servicios evaluados.

Así mismo, esta fase permite además de comprobar las vulnerabilidades sobre las cuales se tiene duda de su existencia, identificar nuevas vulnerabilidades que no hayan sido detectadas por las herramientas automáticas.

Nota: pendiente presentación y aprobación del plan de explotación.

Objetivo

Esta fase tiene como objetivo, la ejecución de los tipos de ataque consignados dentro del plan de hacking ético, los cuáles son ejecutados bajo el esquema de ventanas (si aplica) en las fechas definidas de común acuerdo con la entidad.

FASE 4. Generación y Socialización de Resultados (NO REALIZADA)

Objetivo

Esta fase contempla la elaboración y presentación del informe final, en el cual se consolidan los resultados de las pruebas de vulnerabilidad.

Alcance

Esta fase contempla la consolidación de toda la información recopilada dentro de las pruebas realizadas. Lo anterior permite al cliente conocer el estado final de la evaluación de seguridad técnica sobre la infraestructura, así como corregir dichos hallazgos en el menor tiempo posible.

Entregable

Para esta fase se entregan los siguientes documentos (sin embargo, se alinea con lo requerido dentro del pliego de condiciones y el contrato establecido con la entidad):

a. Informe ejecutivo con los siguientes capítulos:

- Documento con la descripción completa y detallada de la metodología incluyendo la forma en la que se definen los rangos de criticidad de las vulnerabilidades, la identificación de falsos positivos y la categorización de vulnerabilidades reales. La valoración de vulnerabilidades debe considerar la clasificación CVE (Common Vulnerabilities and Exposures).
- Informe sobre las herramientas utilizadas, mecanismos de operación (p. ej. Conexión de un equipo o agente a la red de la **GOBERNACION DEL VALLE DEL CAUCA**, horario de ejecución sugerido, forma de monitoreo, etc) y condiciones de seguridad para evitar indisponibilidad de los servicios.
- Informe de cada prueba que contenga los resultados del análisis de vulnerabilidades, identificando la causa que está generando la vulnerabilidad, los riesgos a los que está expuesta la organización, las alternativas de remediación y la hoja de ruta propuesta para su implementación.

Nota: se presentará una vez se ejecuten las pruebas de ethical hacking.

FASE 5. Prueba de verificación de la remediación (Retest) (NO RELIZADA)

Objetivo

Esta fase contempla la ejecución de prueba de comprobación para el cierre de vulnerabilidades. Esto permite validar que la remediación aplicada sobre las vulnerabilidades sea efectiva.

Alcance

Esta fase incluye la ejecución de los escaneos automáticos o manuales que se ejecutaron para descubrir las vulnerabilidades durante la Fase 1.

Entregable:

Para esta fase se entregan los siguientes documentos:

a. Informe de remediación: Se entregará un informe con el resultado de la verificación de la remediación de vulnerabilidades.

7. NIVELES DE CLASIFICACIÓN

Las vulnerabilidades se clasifican de acuerdo con los siguientes niveles:

Ítem	Descripción
Extremo	La explotación de una vulnerabilidad con nivel Crítico podría proporcionar acceso a datos y sistemas no autorizados, a un nivel de administración. El riesgo contempla la exposición de información sensible, tal como identificadores de usuario (nombres), contraseñas, información propietaria,

	secretos, números de tarjetas de crédito, información de clientes, de colaboradores u otra información sensible de la organización. Así mismo, podría llegar a generar Denegación de Servicio que impacte de manera importante la continuidad de las operaciones.
Alto	La explotación de una vulnerabilidad con nivel Alto podría proporcionar acceso a datos y sistemas no autorizados, en la mayoría de los casos a un nivel administrativo o usuario avanzado
Medio	La explotación de vulnerabilidades con nivel Medio podría permitir indirectamente acceso a archivos de configuración, datos, o afectar parcialmente un sistema de información.
Bajo	Estas vulnerabilidades son de tipo informativo, por ejemplo, las configuraciones de puertos que tienen habilitados y servicios corriendo.

Tabla 1. Niveles de vulnerabilidades

NOTA: De acuerdo con los resultados obtenidos el nivel de riesgo es clasificado por PASSWORD como **EXTREMO.** Los resultados se presentan en el numeral

8. RESULTADOS DE ANÁLISIS DE VULNERABILIDADES

SE ELIMINA POR SER INFORMACIÓN CLASIFICADA