TECNOLÓGICO DE MONTERREY®

Dictámen final sobre
Auditoría de Seguridad Información

Reporte de Pruebas de Penetración

Descripción breve

En este reporte se describe a que plataformas de las requeridas se pudo tener acceso, en qué condiciones y con qué herramientas se hizo dicha prueba. Así también se detalla el método, plataforma y escenario bajo el cual se pudo penetrar a las Plataformas.

Jesús R. González / Juan Arturo Nolazco

jrgonza@gmail.com jnolazco@itesm.mx

Índice

Tabla de Ilustraciones

Versión	Fecha	Descripción
1.0	18 – Mayo – 2017	Resultados del las pruebas de penetración a las aplicaciones requeridas por el IEC. Análisis de vulnerabilidades

Dictamen elaborado por MsC. Jesús Raúl González Hernández en coordinación con Dr. Juan Arturo Nolazco.

1 Resumen Ejecutivo

En este documento se presenta las herramientas y metodología que se utilizó en las pruebas de penetración a las herramientas solicitadas por el IEC.

Se utilizarón herramientas para poder verificar puertas abiertas y explotarlas mediante vulnerabilidades encontradas en los sistemas. Las vulnerabilidades utilizadas para explotarlas están listadas en el documento *REPORTE ESCANEO VULNERABILIDADES* como parte de este entregable.

2 Metodología

Para llevar acabo estas pruebas se baso en el esquema de *Penetration Testing Execution Standard* (PTES - http://www.pentest-standard.org/index.php/Main_Page) adecuado para los requerimientos y alcances de tiempo que se tenían en este análisis. De este modo se siguieron los pasos establecidos de acuerdo al estándar:

- Interacciones de enlace – Se tuvo varias entrevistas para poder entender el modelo de operación y recopilar información del sistema así como de entidades públicas para conocer donde esta ubicada la red, como llegar a ella, direccionamiento (público y privado).
- Reunir inteligencia – Se reunió datos sobre el IEC así como sus conexiones y sistemas a los que esta conectado, públicamente. Esta etapa, por cuestiones de los tiempos de análisis, no se tuvo la profundidad que se debiera haber tenido apra tener una base informativa mas bien estructurada.
- Modelación de riesgos – Mediante entrevistas y cuestionarios, se pudo modelar las amenazas, vulnerabilidades y determinar los riesgos de que se presentaran dichas actividadse bajo un esquema quantitativo.
- Análisis de vulnerabilidades – Se realizó un escaneo con varias plataformas, descritas en secciones posteriores, sobre las plataformas así como sobre algunos procesos que tienen que ver con las elecciones y el conteo a realizar durante Junio 2017
- Explotación de vulnerabilidades – Se utilizarón plataformas automatizadas mediante las cuales se pudiese explotar las vulnerabilidades surgidas en el análisis. Estas herramietnas permiteron que, dado el tiempo con el que se contaba, se pudiera tener un análisis automatizado para poder revisar la infraestructura contenida en el IEC.
- Post Explotación – Durante esta fase se retiene control de los equipos comprometidos para valorar su uso en alguna fase posterior de estudio. Esta fase no se llevo acabo
- Reporte – El reporte que se compone a esta fase es esta sección.

En todo momento se realizaron pruebas donde se valoro la agresividad de las pruebas y minimizo la afectación de la infraestructura y operación del IEC.

2.1 Herramientas

Las herramientas que se escogieron para este proceso son todas de fuente abierta (open-source) las cuales permiten flexibilizar su configuración, en algunos casos aparte de tener un soporte de la comunidad de desarrollo de fuente abierta lo cual permite tener, en ocasiones, un mejor alcance que las herramientas licenciadas y comerciales.

Los programas que se utilizaron para estas pruebas fueron los siguientes

- PING – Detección de elementos en la red
- NMAP – Descubrimiento de hosts y puertos escaneando un rango de IP's
- NCAT – Aseguramiento y validación de puertos disponibles sobre lo encontrado en NMAP
- NIKTO – Pruebas dirigidas particularmente a servicios de web
- OPENVAS – Conjunto de herramientas para explotar las vulnerabilidades disponibles en los puertos y direcciones encontradas por las herramientas anteriores.

La herramienta que se uso con el objetivo de penetrar los hosts, fue la de OPENVAS. A esta herramienta se le cargaron las distintas direcciones IP para escanear y poder buscar explotar las vulnerabilidades encontradas por las otras herramientas.

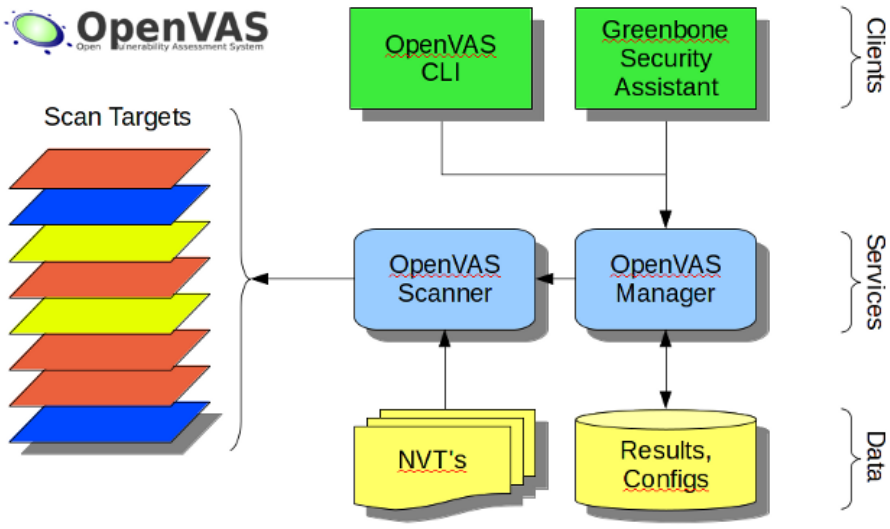

Ilustración 1 Arquitectura de la herramienta de OPENVAS usada para penetración

Los parámetros de cada una de las herramientas se pueden ver en la sección de pruebas de penetración.

2.2 Ambiente

Las pruebas de penetración se llevaron acabo desde afuera de la red del cliente (Internet), no se tuvo acceso a la red desde adentro para realizar la misma prueba.

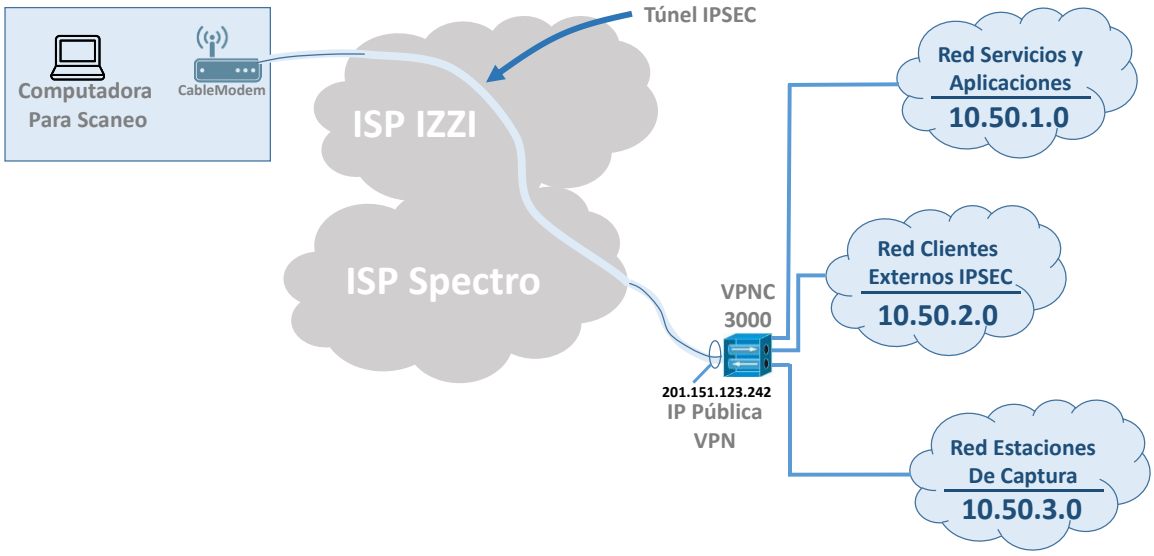

Ilustración 2 Diagrama de conexión para reconocimiento/descubrimiento/penetración

Los scripts y programas se corrieron desde la computadora de Escaneo.

3 Pruebas de penetración

Se realizo las pruebas y se corrieron scripts para las direcciones desde el bloque 10.50.2.0. Fueron varias las direcciones desde donde se ejecutaron ya que se conecto en varios días.

Estas pruebas fueron hechas desde el bloque 10.50.2.0. La computadora que origino los paquetes para la penetración se conecto de forma externa vía IPSEC atravesando un firewall como punto de terminación de túnel a los distintos puertos de las aplicaciones que se encontraron en la fase de escaneo y descubrimiento.

El orden de las pruebas con sus parámetros de configuración para escaneo, previo a la penetración es:

1. **`Ping - ping -c 2 -i2 ip-host`** – se inserta la dirección IP en el host y se configura
   - **`[-c 2 ]`** - numero de envios de icmp a la ip para validar disponibilidad y alcanzabilidad
   - **`[-i2]`** – Tiempo de vida para expirar intentos de conexión
   - **`[ip-host]`** aqui hay una variable que lleva el dato de la ip o host en turno para validar.
2. **`Nmap ip-host`** – Se descubre mediante prueba ligera validar los puertos abiertos, filtrados o cerrados en el host o red.
   - **`[ip-host]`** – Host que se va a analizar. En el caso particular, se definió una red completa (10.50.1.0)

3. **`nmap -T5 -sV -n -O -A -v -Pn -sS -P0 ip-host`** – Este es un escaneo mas agresivo sobre los distintos elementos de la red.
    - **`-T5`** Temporizador nivel 5 (el nivel mas rápido)
    - **`-O`** Habilitar detección de Sistema operativo
    - **`-sV`** probar los puertos abiertos y determiner versión del servicio que usa
    - **`-n/-R`** No resolver vía DNS
    - **`-A`** Habilitar traceroute y detección de Sistema operativo
    - **`-v`** Nivel de salida (los datos que se proporcionan de resultado)
    - **`(-Pn)`** Trata todos los hosts saltando descubrimiento de estos.
    - **`-sS`** escaneo de ventana establecida en TCP SYNC/Connect()/ACK/Window/Scan
    - **`-P0`** Asume disponibilidad en todos los hosts (ejecuta todas las pruebas en todos los hosts)
4. nc ip-host {port} - Netcat toma el host en turno en una rutina de puertos en turno de la list generada con nmap y se conecta a cada puerto en turno obteniendo informacion de servicio
5. nikto -C all -h ip-host -p {puerto} - nikto recive ip-host en turno y de la subrutina de puerto en turno. Realiza detección de malas configuraciones y vulnerabilidades en el servidor objetivo, detección de ficheros en instalaciones por defecto, listado de la estructura del servidor, versiones y fechas de actualizaciones de servidores, tests de vulnerabilidades XSS, ataques de fuerza bruta por diccionario, reportes en formatos txt, csv, html, etc.
6. OPENVAS – bajo esta plataforma se utiliza toda la salida recopilada y se selecciona las vulnerabilidades en la base de datos para poder explotar cada uno de los puertos y servicios que se detectaron abiertos con rutinas y plugins que se tienen ya definidos por la aplicación.

3.1 Resultados

Fue posible establecer durante la parte de escaneo de la red, el inventario de todos los elementos que se estaban revisando y los que se pretendía penetrar, tal y como se puede apreciar en la sección de escaneo y descubrimiento de este proyecto.

Las pruebas se dirigieron a las direcciones en el bloque 10.50.10 donde se encuentran las IP's de las aplicaciones que se están probando:

- 10.50.1.8
- 10.50.1.9
- 10.50.1.10
- 10.50.1.11
- 10.50.1.100
- 10.50.1.101
- 10.50.1.102
- 10.50.1.103
- 10.50.1.104
- 10.50.1.105
- 10.50.1.106
- 10.50.1.107
- 10.50.1.108
- 10.50.1.109
- 10.50.1.110
- 10.50.1.111
- 10.50.1.127
- 10.50.1.128

Las aplicaciones y/o servicios contra lo que se esta probando incluyen, entre otros (puertos más conocidos):

```
TCP 80 – HTTP                    TCP 21 – FTP Control
TCP 443 – SSL                    TCP 22 – SSH
TCP 3306 – MYSQL                 TCP  8086
TCP 2222                         TCP 3000
```

Esto se tiene documentado en una de las evidencias de escaneo en este proyecto

```
Discovered open port 3306/tcp on 10.50.1.101      Discovered open port 80/tcp on 10.50.1.111
Discovered open port 443/tcp on 10.50.1.9         Discovered open port 80/tcp on 10.50.1.103
Discovered open port 443/tcp on 10.50.1.8         Discovered open port 80/tcp on 10.50.1.100
Discovered open port 22/tcp on 10.50.1.8          Discovered open port 80/tcp on 10.50.1.106
Discovered open port 21/tcp on 10.50.1.104        Discovered open port 2222/tcp on 10.50.1.100
Discovered open port 22/tcp on 10.50.1.9          Discovered open port 8086/tcp on 10.50.1.108
Discovered open port 22/tcp on 10.50.1.10         Discovered open port 17988/tcp on 10.50.1.9
Discovered open port 80/tcp on 10.50.1.8          Discovered open port 3000/tcp on 10.50.1.109
Discovered open port 22/tcp on 10.50.1.11         Discovered open port 17988/tcp on 10.50.1.8
Discovered open port 80/tcp on 10.50.1.9          Discovered open port 8088/tcp on 10.50.1.108
```

Al intentar penetrar los sistemas del IEC esto no fue posible. Análisis mas detallado lleva a deducir que existe un regulador de tráfico que no permite hacer las rondas de ataque desde la conexión en IPSEC. Como se muestra en el reporte de OpenVas, no hay resultados de riesgo para ninguna de las instalaciones en la red 10.50.1.0 donde se encuentran los servicios y aplicaciones del PREP del IEC.

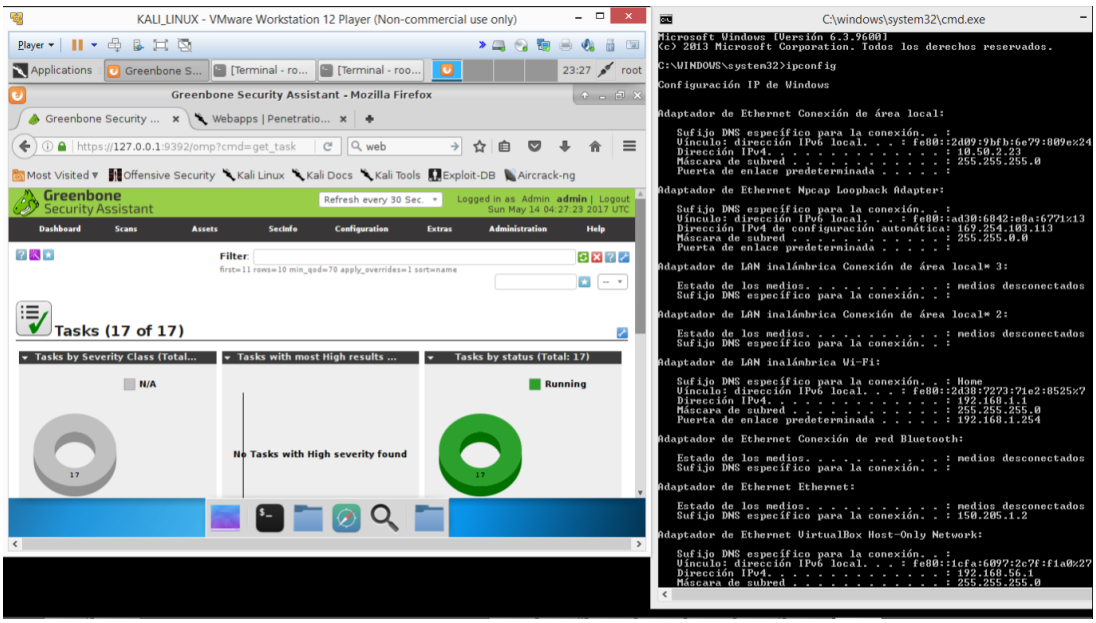

Ilustración 3 Terminación de pruebas de penetración

Lo que se encontró, como se puede ver en las imágenes, es que no hubo resultados. Esto se debe a que no es posible penetrar los puertos abiertos que se encontraron en los distintos servidores del IEC sobre la red 10.50.1.0.

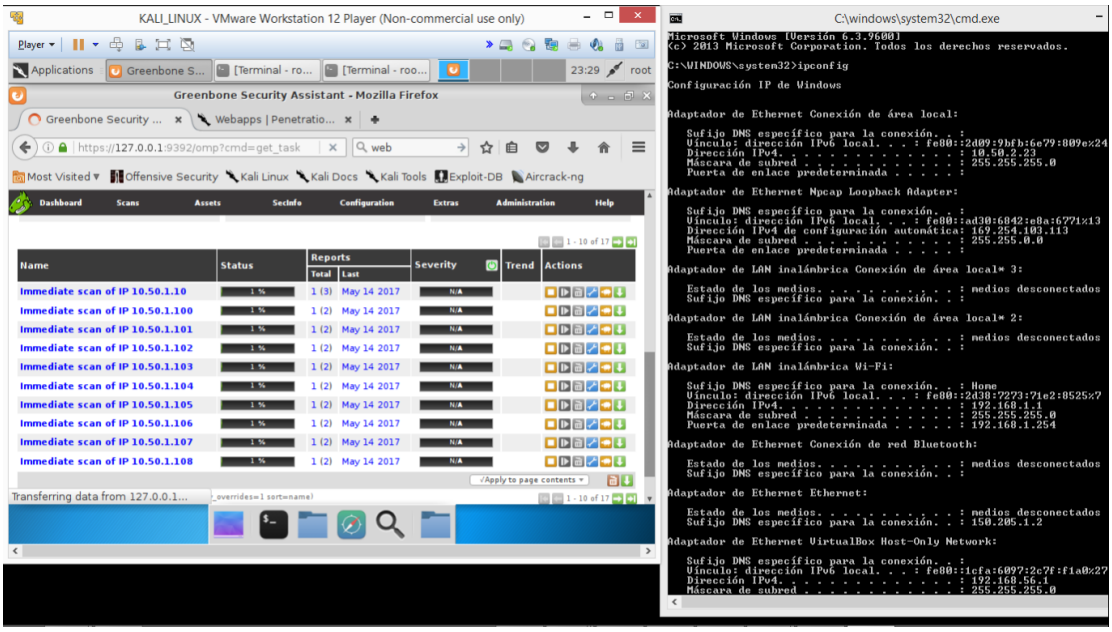

Ilustración 4 1er Grupo de tareas para ejecutar en pruebas de penetración

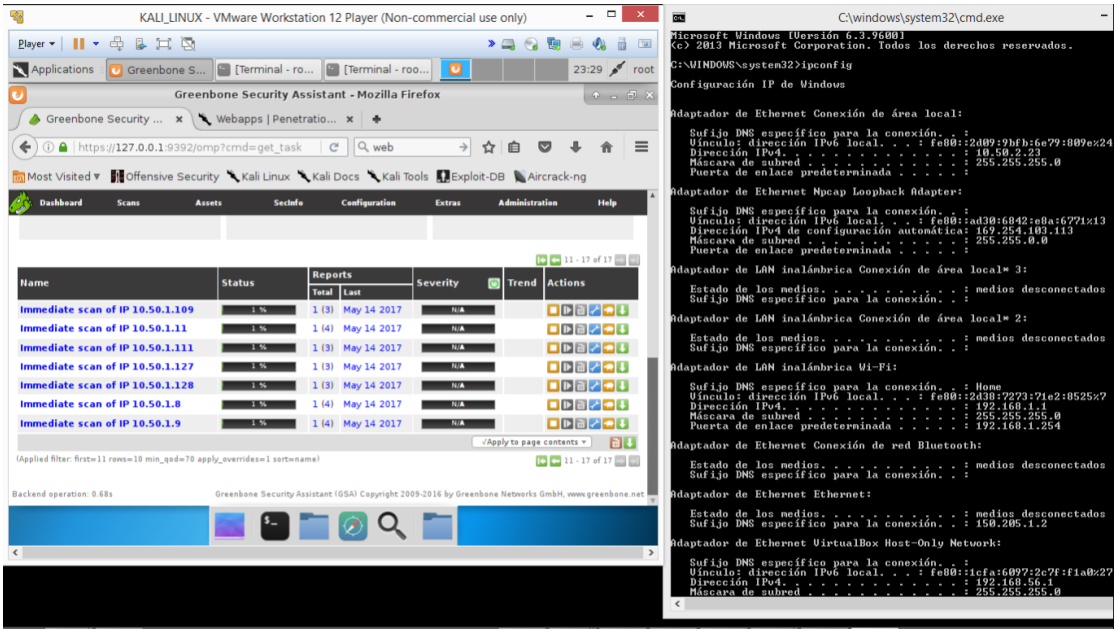

Ilustración 5 2o Grupo de tareas para ejecutar en pruebas de penetración

Después de revisar la arquitectura de red a la que nos conectamos, los elementos que existen la configuración y haciendo un análisis sobre la terminación del túnel en el VPN Concentrator; se puede ver que en el VPN Concentrator, que es en el terminador del túnel de IPSEC, esta basado en el Software del Firewall PIX OS 8.4.

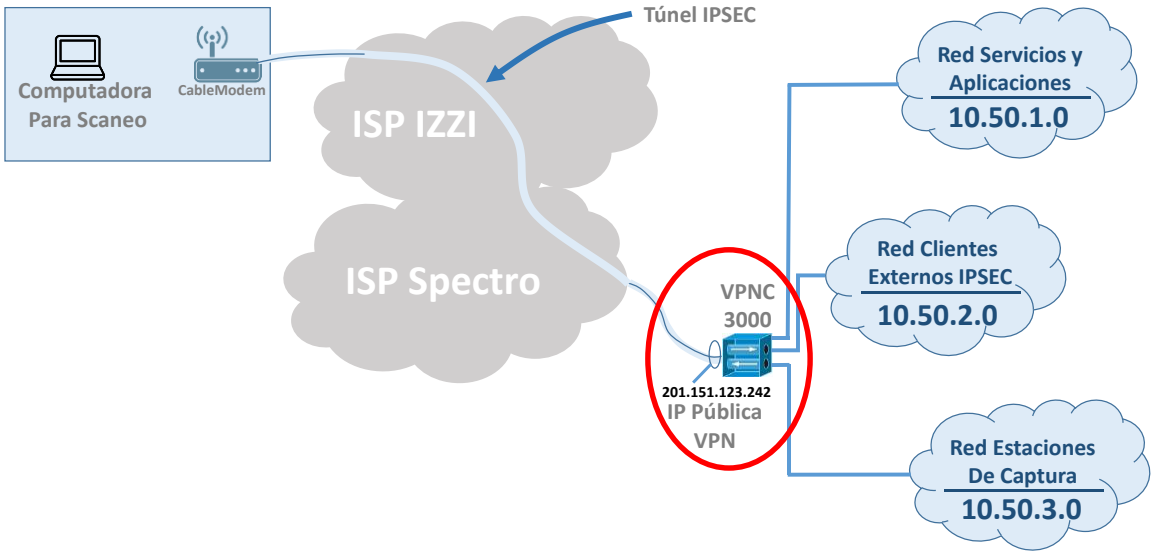

Ilustración 6 Diagrama de conexión para penetración

Este elemento de red tiene una funcionalidad de limitación de tráfico por protocolo haciendo uso del comando **`fixup protocol`** el cual esta habilitado por definición y que marca para inspección los paquetes del protocolo que se configure en el comando para revisarlos en detalle **.** Este comando es una forma en que el VPNC controla las sesiones dirigidas a puertos tomando en cuenta:

- Puerto de llegada – De donde viene la conexión
- Comandos – Dialogo que se esta estableciendo entre las dos entidades para restringir las respuestas hacia el elemento externo
- Cambios en el puerto – redireccionamientos de puerto hacia otro para cuestiones de seguridad hacia atrás del host, donde se esta protegiendo.

Estos comandos funcioan en las dos direcciones del equipo. Mas información sobe este comando se puede obtener directamente de CISCO:

http://www.cisco.com/en/US/docs/security/pix/pix50/configuration/guide/commands.html#wp5788

4 Conclusiones

El resguardo de la infraestructura del IEC desde fuentes externas (Internet) se encuentra cubierto mediante el control de conexión en el terminador de tuneles, lo cual disminuye el riesgo de escaneos así como explotación de vulnerabilidades debido al control de protocolos que se tiene habilitado con la función en el VPNC.

Aunque la amenaza de que alguien pueda entrar a la red y entrar directamente hacia alguna de las aplicaciones existe, la probabilidad de que esto suceda se considera baja debido a:

- Requerimientos de conocimiento de la infraestructura y arquitectura de la red que la persona debe tener para entrar, conocer que aplicaciones hay para saber usarlas. Esto en adición que dicho usario deberá contar con un usuario y clave para entrar por el VPNC vía IPSEC por lo que si esto llegar a darse, sería probablemente una persona interna o con conocimiento del administrador quien otorgo permisos de acceso para que esto se diera.
- Controles aplicados de acceso a la red. De forma remota se ve difícil que pueda explotar algo dado el control que se tiene en el VPNC para limitar manejo y manipulación de puertos. Aun así, los controles para limitación de uso y acceos a las bases de datos que se documentan en la sección de recomendaciones minimizarán el riesgo que esta situación pueda darse.
- Usuarios con acceso limitados en cuanto a su actividad adentro de la red. El acceso de usuarios a la red de forma remota para cualquiera de los procesos que se tienen en firme, debe ser limitado y no ser único para todas las aplicaciones. Con esta medida se disminuirá el riesgo de explotación en las aplicaciones.

Las vulnerabilidades existentes en las aplicaciones y servidores, no se pudieron explotar vía conexión externa por el control que debe estar habilitado en el concentrador de VPN que se tiene instalado.

Análisis interno de la infraestructura no fue posible realizarse debido a los tiempos establecidos para su ejecución.

4.1 Trabajos futuros

Como proyecto futuro, se podría hacer una explotación controlada desde adentro de la red del IEC para validar la facilidad de explotar vulnerabilidades desde adentro de la red. Esto, aunque poco probable ya que tendría que ser alguien interno, se considera relevante para validación de los sistemas en una forma integral.