TECNOLÓGICO DE MONTERREY®

Instituto Electoral Coahuila

Dictamen Final Auditoría Seguridad de Información

Mayo 2017

Jesús R. González / Juan Arturo Nolazco
jrgonza@gmail.com jnolazco@itesm.mx

Tecnológico de Monterrey

IEC
Instituto Electoral de Coahuila

Alcances de la auditoría seguridad

- El IEC solicito una auditoría a los sistemas del PREP para asegurar su continuidad operativa durante el proceso electoral de Junio del 2017 así como ver los riesgos de en los elementos y aplicaciones involucrados así como los de procesos asociados a las aplicaciones.

- La solicitud de los análisis fue sobre las aplicaciones ubicadas en el IEC que usan para el proceso electoral describiendo las herramientas y lo que se utilizo para estas pruebas. Las herramientas se describen así:
  - Servidor de WEB Apache
  - Servidor WEBDav
  - Base de datos MYSQL
  - Desarrollos hechos internamente en MongoDB, PHP, Python
  - Sistemas operativos UBUNTU 16.04

- Se solicito el análisis también de la infraestructura de redes describiendo las herramientas usadas para descubrir vulnerabilidades y los pasos que se utilizaron para ejecutarlas.

Tecnológico de Monterrey

IEC
Instituto Electoral de Coahuila

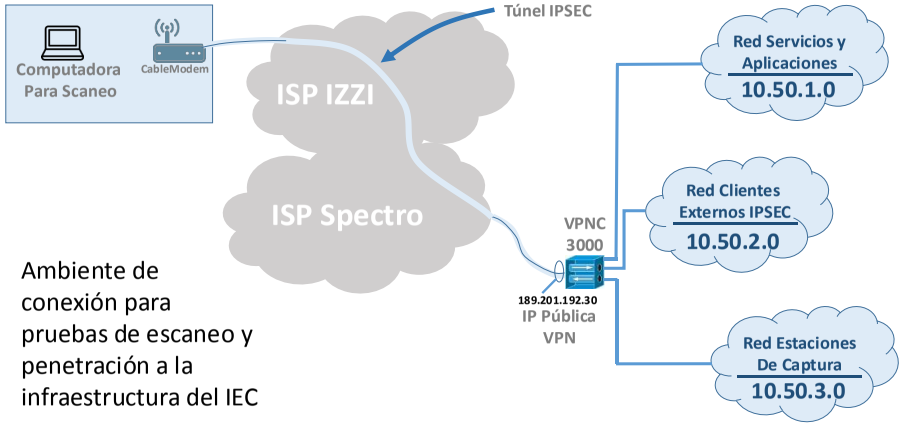
Metodología

- Se manejo la metodología de *Penetration Testing Execution Standard* (PTES - http://www.pentest-standard.org/index.php/Main_Page)
  - Interacciones de enlace – Se tuvo reuniones con distintas personas involucradas en la operación de la infraestructura para entender el modelo de operación y recopilar información del sistema
  - Reunir inteligencia- Reunión de información sobre la´conexión de la red del IEC así como sus interacciones hacia afuera e internas
  - Modelación de riesgos- Mediante entrevistas y cuestionarios, se pudo modelar las amenazas, vulnerabilidades para determinar riesgos
  - Análisis de vulnerabilidades - Se realizó un escaneo con varias plataformas, así como investigación de versiones de SW instaladas
  - Explotación de vulnerabilidades – Se utilizaron plataformas para explotar vulnerabilidades de forma automática. Esto se hizo de forma remota conectando las plataformas al sitio con IPSEC para el análisis.
  - Post Explotación – Esta fase consta de retener el control de equipos para valorar su uso para fines posteriores en función de la importancia y relevancia de la información que se tiene
  - Reporte – El reporte que se esta entregando como resultado del análisis.

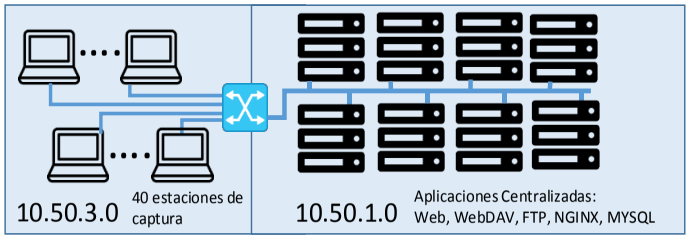
- Para el proceso de análisis de riesgos y su documentación se utilizo el estándar NIST 800-30 (http://csrc.nist.gov/publications/PubsSPs.html#800-30) normando cualitativamente los impactos y probabilidades para determinar su riesgo.

Descubrimiento

- El descubrimiento de las redes donde están ubicados los objetivos se hizo desde una conexión remota vía IPSEC para lo cual se descubrieron las siguientes redes
  - 10.50.1.0 – Red donde están los servicios y aplicaciones
  - 10.50.2.0 – Red de clientes externos IPSEC que se conectarán de forma dinámica para vaciar resultados
  - 10.50.3.0 – Red de las estaciones de captura
- Las herramientas usadas para descubrir la red son:
  - NCAT – Abre conexiones a puertos TCP/UDP en un host
  - ZENMAP – Permite automatizar el recorrido de direcciones IP descubriendo puertos y servicios instalados
  - ANGRYPING – Permite hacer pings de forma automática a varios hosts mostrando servicios habilitados en cada host
  - TRACERT – Con esta herramienta nos permite trazar rutas de un origen a un destino mostrando el camino que sigue



Ambiente de conexión para pruebas de escaneo y penetración a la infraestructura del IEC



Ambiente interno de conexión de las distintas redes en el IEC.

La red 10.50.2.0 es en donde se conecta el túnel de IPSEC, no había nadie conectado

Tecnológico de Monterrey

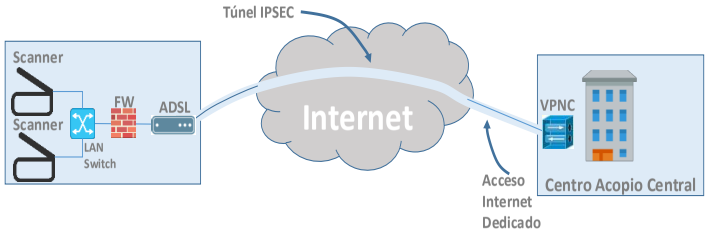
IEC
Instituto Electoral de Coahuila

Descubrimiento

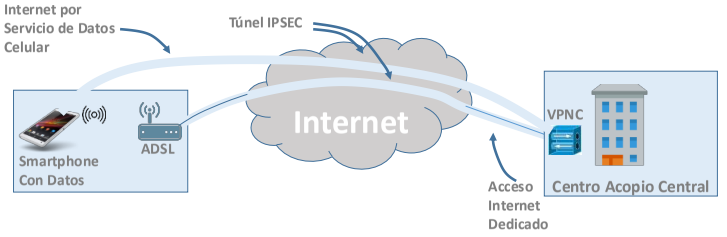
- La red 10.50.2.0 se usará para recibir conexiones vía IPSEC de los distintos sitios de acopio remotos en dos escenarios:
  - Equipados con infraestructura de escáneres EPSON y se conectarán vía enlaces de internet asimétricos los cuales realizarán conexiones IPSEC con un FW Fortinet hacia el centro de acopio central en Saltillo (Este escenario es para los sitios mas grandes).
  - Tomarán fotografías con un celular para enviarlas vía IPSEC hacia los el centro de acopio central en Saltillo. Todo esto montado con aplicaciones en el Smartphone.

- La red 10.50.4.0 se utilizará (no estaba implementada al momento del análisis por lo que no se escaneo ni analizo) para interconectar la infraestructura de aplicaciones a un centro de datos (Rackspace) para respaldo en caso de algún incidente

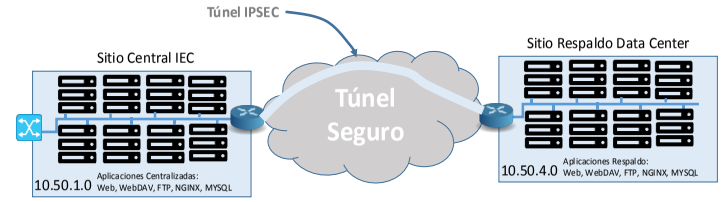
Sitio Acopio con escáner



Sitio Acopio con Smartphone



Interconexión planeada a un centro de datos para respaldo



Tecnológico de Monterrey

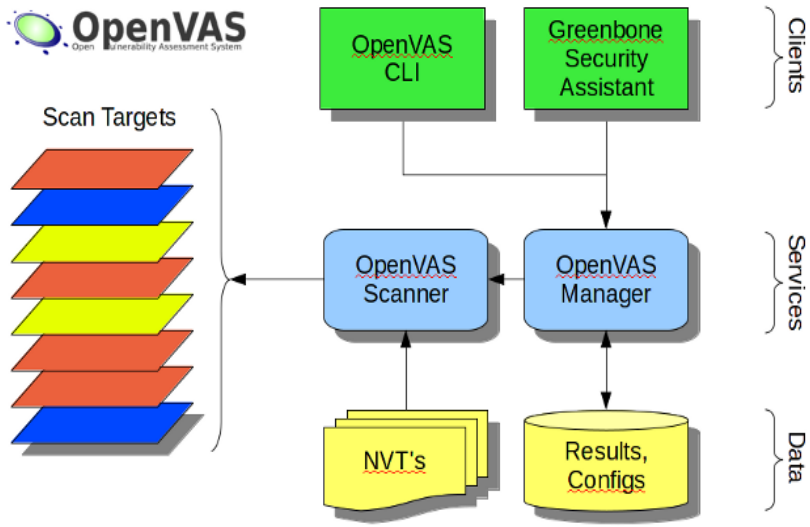
IEC
Instituto Electoral de Coahuila

Vulnerabilidades

- En la red de aplicaciones (10.50.1.0) se encontraron vulnerabilidades asociadas a las aplicaciones y algunos servicios en dos partes
  - Análisis de las versiones:
    - Se hizo un análisis en la NVDB (https://nvd.nist.gov/vuln) basado en los sistemas y servicios instalados con las versiones correspondientes, y se encontró 17 vulnerabilidades de nivel alto y medio y solo una de nivel crítico.
    - En análisis de vulnerabilidades corrido sobre las aplicaciones no se encontró evidencia de estas vulnerabilidades
  - Escaneo de las aplicaciones:
    - En esta etapa se encontraron 7 vulnerabilidades de la OSVDB, debido a la herramienta que se utilizo y se mapearon 3 de ellas a las de la base de datos de NVDB
    - Las 7 vulnerabilidades estan catalogadas de nivel medio y alto (no mas de 7.5 en escala de 10)
- En las redes 10.50.2.0 (conexiones de IPSEC de sitios remotos) así como en la 10.50.3.0 no se encontró vulnerabilidades ya que al momento de escanear, no había elementos encendidos para escanear
  - La red 10.50.2.0 no había otro sito conectado al momento
  - La red 10.50.3.0 No había estaciones de captura encendidas al momento de hacer el escaneo.
- Se hizo una entrevista con los encargados del proceso electoral y en base a esta se revisaron procesos de contabilidad así como de captura en todo el proceso y se identificaron algunas vulnerabilidades en los procesos.
  - 12 vulnerabilidades en los procesos de captura en los sitios remotos de acopio así como en el sito central en saltillo
  - 11 vulnerabilidades en la operación central del proceso electoral

Pruebas de Penetración

- Para las pruebas de penetración se realizaron utilizando las herramientas siguientes:
  - PING – Detección de elementos en la red
  - NMAP – Descubrimiento de hosts y puertos en 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 – Colección de herramientas para explotar vulnerabilidades disponibles en direcciones puertos encontrados
- La herramienta para ataque a vulnerabilidades usada fue OPENVAS y NIKTO las cuales en función de las vulnerabilidades obtenidas las explota.
  - Las direcciones escaneadas son de la red 10.50.1.0
  - La comprobación de la corrida se hizo, aparte de OPENVAS usando las herramientas por separado.



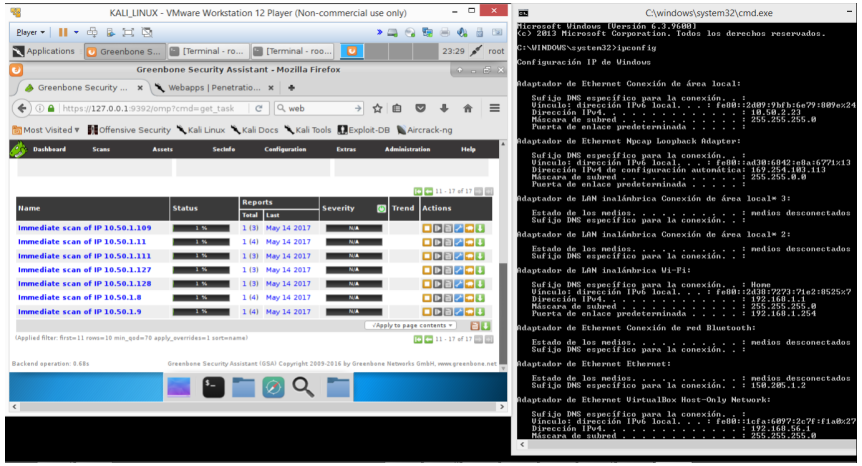
- 10.50.1.8
- 10.50.1.9
- 10.50.1.10
- 10.50.1.11
- 10.50.1.100
- 10.50.1.101
- 10.50.1.102
- 10.50.1.103
- 10.50.1.104
- 10.50.1.105
- 10.50.1.106
- 10.50.1.107
- 10.50.1.108
- 10.50.1.109
- 10.50.1.110
- 10.50.1.111
- 10.50.1.127
- 10.50.1.128

Tecnológico de Monterrey

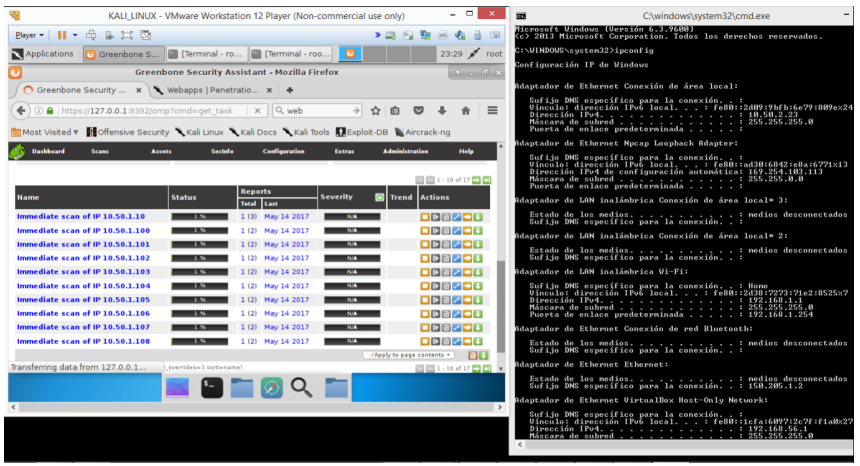
IEC Instituto Electoral de Coahuila

Pruebas de Penetración

- Al lanzar las herramienta de OPENVAS se encontró que no fue posible explotar los puertos de servicios que se encontraron abiertos a pesar que se recorrieron manualmente las pruebas como se muestra en la evidencia en la sección de anexos.



- Dado que no fue posible explotar los puertos, el VPN Concentrator debe tener configurado un regulador
- El regulador de tráficose configura en forma de la funcionalidad FIXUP PROTOCO* de Cisco que limita las operaciones hacia los puertos de servicios



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

Tecnológico de Monterrey

IEC Instituto Electoral de Coahuila

Modelación de Riesgos

- Se utilizo un esquema cualitativo de clasificación de riesgos donde en función del impacto y probabilidad, se determino la dimensión del impacto.
  - Esto se puede observar en el mapa de calor con el cual se revisaron las tablas de amenazas y vulnerabilidades para en base a que tan probable es que suceda y el impacto que este tenga determinar el riesgo.
- Se modelaron los riesgos utilizando las vulnerabilidades encontradas y amenazas observadas durante el estudio
  - 22 riesgos de procesos de los cuales ninguno resulto Muy Alto
  - 37 riesgos tecnológicos de los cuales ninguno resulto Muy Alto
- Los riesgos de las vulnerabilidades escaneadas que fueron 13, todos resultaron Medios
  - Esto en base a que el tipo de vulnerabilidad y amenaza que se deben presentar requieren un alto conocimiento técnico y que solo se podrían explotar estando internamente en la red.

Impacto	Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Mul Alto	Medio	Alto	Alto	Muy Alto	Muy Alto
Alto	Bajo	Medio	Alto	Alto	Muy Alto
Medio	Bajo	Medio	Medio	Alto	Alto
Bajo	Muy Bajo	Bajo	Medio	Medio	Alto
Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo	Medio

- Los riesgos encontrados con esa calificación es una fotografía al momento que se realizo el análisis y que en un futuro podrá ser analizada para ver la disminución de las vulnerabilidades encontradas

Tecnológico de Monterrey

IEC Instituto Electoral de Coahuila

Recomendaciones

- En base a la modelación de riesgos se plantearon los controles para mitigar el riesgo que se esta presentando por la vulnerabilidad y probabilidad de que sea explotada.

- Los controles que se definieron son:
  - 18 controles de proceso – De estos hay 14 controles que ya existen para las 22 vulnerabilidades analizadas y 8 de las restantes vulnerabilidades son controles que actualmente están en desarrollo por parte del IEC y en base a las entrevistas que se tuvo, se confirmo por parte de los responsables de TI y seguridad que estarían implementados para antes del 4 de junio.
  - 23 controles tecnológicos – De los cuales hay 14 controles ya existentes y 10 están en desarrollo según se aseguro en las entrevistas.

- Entre otras recomendaciones para el IEC, se tienen las siguientes para tomar en cuenta:

Recomendaciones Procesales	Recomendaciones Tecnológicas
• Puntos de revisión • Restricción de acceso • Acceso con artículos personales. • Asegurar niveles de servicio con proveedores de tecnología o servicios • Matriz de responsables • Desarrollo de manual de procedimientos para captura y toma de fotos o escaneo. Esto para los centros de acopio	• Configuración del túnel sin Split Tunnel • Mantener configuración de Fixup Protocol • Centro de datos de respaldo (en desarrollo) • Portal de quiosco en vez de sistema operativo para maquinas de captura. • Actualizar versiones de SW con las vulnerabilidades sin evidencia • Estaciones de captura sin acceso a Internet

Tecnológico de Monterrey

IEC
Instituto Electoral de Coahuila