INFORME PRELIMINAR DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO

- Introducción

El presente documento tiene como objetivo el evaluar la integridad del en el procesamiento de la información y la generación de resultados preliminares dentro de un ambiente controlado y homólogo al que se utilizará en la elección local el día de la jornada electoral.

- Metodología

Utilizando los sistemas de la empresa Informática Electoral, la empresa ejemplifico solamente dos casos de prueba (un caso con el flujo sin errores y otro con error en la validación) para analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, considerando la digitalización, captura, verificación y publicación de resultados, mediante flujos completos e interacción entre los diversos módulos.

Se inicio con la verificación del cumplimiento de las especificaciones funcionales y requerimientos contenidos en el Reglamento de Elecciones del Instituto Nacional Electoral y sus Anexos 13 y 18.5.

Se inicio con la verificación de la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

Se realizó un análisis documental de los módulos y del sistema proporcionado por la empresa.

- Criterios utilizados para la auditoria

Los marcados por el protocolo de Auditoria del Sistema informático del PREP UNAM Version 5 del 23 de enero de 2018. Los cuales cumplen con lo marcados con Reglamento de Elecciones del Instituto Nacional Electoral y sus Anexos 13 y 18.5

- Metodología para clasificar los hallazgos

Como resultado de la revisión de cafa negra se sugiere que los hallazgos sean documentados considerando los siguientes elementos mínimos:

a. Identificador del hallazgo. (número consecutivo)
b. Descripción de la observación.
c. Nivel de impacto.

- Observaciones y recomendaciones

1. Mediante la información documental, no se encontraron hallazgos en la misma. Recomendación: cotejar las observaciones detectadas en los documentos en la visita de finales de mayo con la maqueta de pruebas.

2. No se ha proporcionado acceso a los sistemas MCAD, CAPREP, VERIPREP y SIPREP, de tal manera que se pueda realizar el análisis completo de caja negra para determinar hallazgos en el sistema. Recomendación: Dar acceso remoto a los sistemas que así lo permitan o en su defecto realizar pruebas por casos marcados en el protocolo de auditorias de del Sistema informático del PREP UNAM Version 5 del 23 de enero de 2018, durante la visita de finales de mayo.

3. Dado que las pruebas se realizaron en la empresa y solo se participo como observador, no se lograron analizar todo requerido en el protocolo de Auditoria.

- Conclusiones

No hay suficiente información para considerar que se ha cubierto el análisis de caja negra.
En la información documental la información no se pueden clasificar como hallazgos pues es necesario cotejar las observaciones encontradas con la evidencia real.
Hasta tener acceso a los modulos en una maqueta de pruebas se podrá registrar hallazgos para atender.

INFORME PRELIMINAR DE LAS PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA Y DE LA REVISIÓN DE CONFIGURACIONES DE INFRAESTRUCTURA.

- Resumen ejecutivo

Utilizando el software Nessus Profesional se realizó un escaneo para establecer los activos sobre los que se realizarán las pruebas y la revisión de configuraciones. Se consideraron los siguientes aspectos: clasificación de los activos por funcionalidad y aspectos técnicos; condiciones de operación actual de los activos a evaluar.

Para los horarios de pruebas se considero el horario de servicio de COPREP y de los CATD.

Una vez determinado lo anterior, se designaron los activos primordiales a revisar.

El servicio de pruebas de penetración y análisis de vulnerabilidad para la infraestructura tecnológica tiene como objeto obtener información relacionada con los activos evaluados, conocer el nivel de exposición de información sensible y documentar los hallazgos.

La primera etapa de las pruebas consisten en la identificación de vulnerabilidad en objetivos específicos, así como en otros que podrían proporcionar acceso a ello, intentando explotar vulnerabilidad identificadas para determinar el impacto potencial en caso de que alguna fuera aprovechada por un usuario malintencionado. El tiempo de pruebas para cada uno de los activos es limitado, por lo que se definió un plan de pruebas. Entre las vulnerabilidad que tratan de explorarse se encuentran:

1. Instalaciones por defecto

2. Errores o huecos de seguridad en el software.

3. configuraciones débiles o vulnerables

4. Vulnerabilidades que permiten al atacante remoto acceder de forma no autorizada a información sensible.

5. Vulnerabilidades que permitan al atacante remoto modificar de forma no autorizada el contenido o la visualización del mismo en un activo de información.

6. Vulnerabilidades que provoquen afectaciones a la disponibilidad de los recursos de TIC

7. Modificaciones no autorizadas en el contenido de repositorios de documentos (Base de Datos)

8. Verificación de cuentas son algo tipo de autenticación, cuentas por defecto y contraseñas débiles por medio de ataques de diccionario o fuerza bruta.

Para las pruebas de penetración se consideran dos escenarios:pruebas externas y pruebas internas. En las pruebas externas se evalúan lo objetivos que pueden ser accedido desde internet y se ejecutan a través de este mismo medio desde ubicaciones externas ala organización; las pruebas internas incluyen los objetivos que son accesibles solo desde la red interna y se ejecuta en las instalaciones de la organización.

La revisión de las configuraciones de la infraestructura incluye las visitas a los CATD y la determinación de pruebas de conectividad, en VPNs, Firewalls, etc.

- Alcance

Las Pruebas se realizaron de forma Interna en las instalaciones del COPREP, y los CATD 13, 14 y 18.

- Resultado de las pruebas

Los resultados de las pruebas se entregaron como anexos en html para cada uno de los lugares asignados.

- Recomendaciones generales de las pruebas de penetración

En términos generales las maquinas que participan en el PREP se encontró que en su mayoría deben atenderse con las actualizaciones del sistema, pues no presentaron vulnerabilidad en los otros rubros marcados.

Se debe atender de manera especifica los análisis marcados como:

A. CATD13Digitalizador, ya que muestra información que puede convertirse en un hallazgo de riesgo alto si no se atiende cuando se realice el análisis de forma externa, esto se repite en cada uno de los CATD pero genero un reporte por separado para que se mostraran como ejemplo a la empresa Informática Electoral.

B. COPREP10, maquina 10.1.0.201, es primordial atender los hallazgos marcados como altos.

C. COPREP10, maquina 10.1.0.15, es recomendable cambiar el sistema o actualizarlo para evitar los problemas presentados, aunque este equipo no contiene ninguna información del PREP, si puede ser un punto de acceso remoto para algún atacante.

D. Para todo los rubros marcados en Medio se le sugiere realizar una análisis para mitigar tantos como sea posible, o documentar las desiciones sobre las mismas para asumir los riesgos.

- Hallazgos y recomendaciones para las configuraciones de infraestructura.

1. Configuración de los firewalls en los CATD. Se sugiere cambiar la configuración de los firewall instalados en los CATD de acuerdo con la mostrada al responsable de la configuración de los mismos.
2. Infraestructura no perteneciente al PREP en los CATD. Se detectaron cables de red que salen de las oficinas del PREP en dos de los CATD, así como equipos de red no utilizados en las instalaciones de los mismos, se sugiere eliminar infraestructura que no pertenezca a los mismos.
3. Balanceador. Considerar incluir un balanceador en la infraestructura del COPREP.

Es necesario terminar al menos 12 CATD para determinar que se han atendido las sugerencias indicadas.

Anexos:
COPREP10.html
COPREPVMW.html
COPREPWeb.html
CATD13.html
CATD13Digitalizadores.html
CATD14.html
CATD18brother.html
CATD18Digitalizador.html
CATD18Sin.html
Memoria Fotografica inicial

Atentamente

M en C Guillermo Vázquez Sánchez