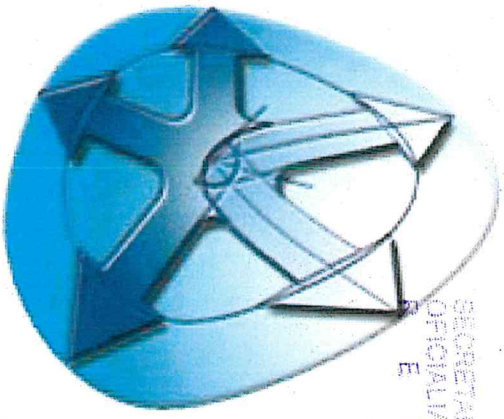
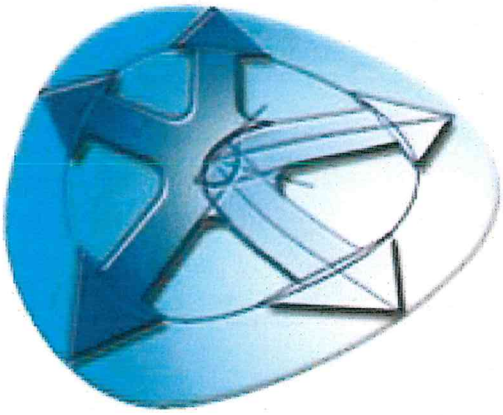


Informe Final de Auditoría al Programa de Resulados Electorales Preliminares del Instituto Electoral del Estado de Querétaro

2018

Entregado en hoja impresa y en medio magnético



Informe Final de Auditoría al Programa de Resulados Electorales Preliminares del Instituto Electoral del Estado de Querétaro

2018

INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO PREP QUERÉTARO

- Introducción

El presente documento tiene como objetivo el evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares que se utilizará en la elección local, el día de la jornada electoral.
Estas pruebas permiten conocer el conjunto de condiciones de entrada que ejerciten todos los requisitos funcionales del PREP. En ellas se ignora la estructura de control, concentrándose en los requisitos funcionales del sistema y ejercitándolos. Es decir, se basa en verificar que los datos de entrada (plasmados en las AEC) sean los que se reflejan en la publicación, Pagina Web Publica del PREP.

- Metodología

La revisión se realizó en tres etapas para analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, priorizando la digitalización, captura, verificación y publicación de resultados, determinando los flujos completos e interacción entre los diversos módulos. Para el caso del Instituto Electoral del Estado de Querétaro (IEEQ) son: acopio, digitalización, captura, verificación, y publicación, debiendo cumplirse cada una de ellas en el orden señalado.
Se utilizaron Casos de Prueba considerando los procesos declarados para cada módulo.

- Criterios utilizados para la auditoría

Los marcados por el protocolo de Auditoría del Sistema informático del PREP UNAM, Versión 5, del 23 de enero de 2018.

- Resumen Ejecutivo

Se utilizaron los equipos instalados por el instituto en el CATD Municipal de Corregidora, y se permitió acceso incluso a los servidores para las pruebas de los modulos de Digitalización, Captura y Validación y de Publicación de Resultados.
Se aplicaron los casos de prueba para cada módulo, donde se detectaron problemas la descarga de la base de datos, y de identificación en algunos rubros de identificación del acta. Dichos problemas se corrigieron en el tiempo establecido para el Instituto.
Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en el CATD Distrital 6 el modulo de digitalización y en las oficinas del CCV los módulos de captura, verificación y publicación.
Dos días antes del segundo simulacro se determinó que era necesario en el CCV Alterno, la actualización y reconfiguración de la VPN en varios equipos, la mitigación de dichos hallazgos se demostró dos días después del tercer simulacro.

Así mismo, problemas que se presentaron en la captura de algunos CATD Municipales, se debieron a problemas de infraestructura de telecomunicaciones y no de funcionalidad, es decir la velocidad es baja pero el sistema puede seguir funcionando con en el enlace alterno.

- Resultados

El sistema informático permite la captura, digitalización y publicación de los datos asentados en la Actas de Escrutinio y Cómputo que se reciben en los Centros de Acopio y Transmisión de Datos.

El sistema informático integra los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones, en el marco de la normatividad vigente.

El sistema informático apoya las funciones en los CATD.

Se maneja la Integridad en el registro de la información. Que a partir de un Acta de Escrutinio y Cómputo en papel, se genera una imagen digital completa y legible de ésta y es almacenada sin alteraciones en su contenido y publicada para consulta. Que la imagen digital del Acta de Escrutinio y Cómputo, así como sus datos capturados manualmente son debidamente asociados a la casilla, sección y distrito que corresponda. Que los resultados del Acta de Escrutinio y Cómputo capturados son asociados fielmente al partido, coalición o rubro en el cual se registren.

Para la revisión de desempeño se considerará el universo válido de información de un distrito muestra: únicamente se verificó que el sistema implemente dicha validación o restricción a partir de un catálogo de información el cual deberá tener cargada previamente la información de las casillas válidas.

También se consideró la Contabilización de actas y presentación de resultados acumulados.

Por lo que se considera adecuado para operar el día de la jornada electoral.

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

- Resumen ejecutivo

Las pruebas realizadas consisten en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, y posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar así el impacto que tienen sobre la infraestructura, determinar el nivel de exposición de información sensible.

Evaluar la configuración actual de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática.

La revisión de configuraciones se enfoca en el sistema operativo de servidores, consolas y dispositivos, por lo que no considera los servicios y aplicaciones que se ejecuten en los mismos. Así mismo se verificó la velocidad de las conexiones de internet y que se contara con una conexión de respaldo para el envío de datos.

Todos los hallazgos y oportunidades de mejora que se obtienen, como resultado de la ejecución del pentest y de la revisión de configuraciones, se analizan y se clasifican.

A partir de los informes de las pruebas de penetración y de la revisión de configuraciones, se verificó la aplicación de las medidas de mitigación aplicadas por el Instituto a fin de identificar la persistencia de los hallazgos reportados en la infraestructura de TI.

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.
Una vez determinados los activos a analizar, se utilizaron además las siguientes herramientas para el pentest: OWASPZAP 2.7, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest.

Para los horarios de pruebas se consideró el horario de servicio de los consejos 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 información del PREP, 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 explotarse se encuentran:

1. Instalaciones por defecto
2. Errores o huecos de seguridad en el software.
3. configuraciones débiles o vulnerables
4. Vulnerabilidades que permiten a un atacante remoto acceder de forma no autorizada a información sensible.
5. Vulnerabilidades que permitan a un 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 sin algún 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 éste mismo medio desde ubicaciones externas a la organización; las pruebas internas incluyen los objetivos que son accesibles sólo desde la red interna y se ejecuta, en las instalaciones de la organización.

- Alcance

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

Para la revisión de la infraestructura se revisaron las instalaciones primero como una muestra para la configuración de todos los demás en el CATD Municipal de Corregidora, el cual fue revisado varias veces hasta que las configuraciónes cumplían con los criterios de auditoria. Posteriormente se verificaron los CATD ubicados en los 15 Consejos Distritales y 12 Municipales, CCV Principal, CCV de Respaldo, las instalaciones del IEEQ, y los servidores en la nube.

- Resultado de la Verificación.

Se atendieron los hallazgos de manera satisfactoria en materia de configuraciones de infraestructura y, las pruebas de penetración determinaron que la infraestructura es adecuada para operar en un riesgo bajo.

Cabe aclarar que esta revisión se basa en clasificación de riesgos, y la auditoria pretende mitigar al máximo los hallazgos que se encontraron. Sin embargo la tecnología avanza rápidamente día con día y nuestra estimación no implica que se llegue a un 0% de riesgo.

El siguiente es un compilado fotográfico de los lugares donde se realizó revisión de infraestructura.


IEEQ
CONSEJO DISTRITAL 07
CORREGIDORA


IEEQ
CONSEJO DISTRITAL 08
SAN JUAN DEL RÍO
PROCESO ELECTORAL LOCAL
www.ieeq.mx


IEEQ
CONSEJO DISTRITAL 09
SAN JUAN DEL RÍO
www.ieeq.mx
01 800 400 2003

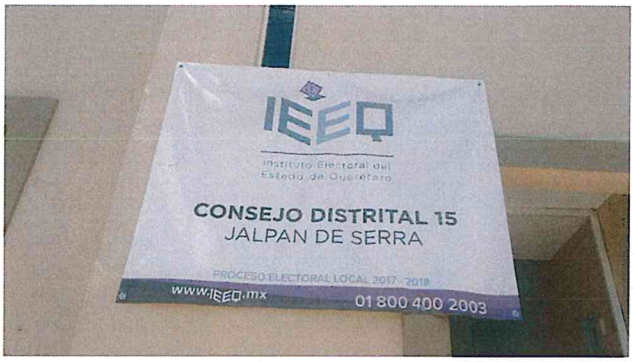

IEEQ
CONSEJO DISTRITAL 10
PEDRO ESCOBEDO


IEEQ
Instituto Electoral del
Estado de Querétaro
CONSEJO DISTRITAL 11
TEQUISQUIAPAN
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


IEEQ
Instituto Electoral del
Estado de Queretaro
CONSEJO DISTRITAL 13
QUERÉTARO
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


IEEQ
CONSEJO DISTRITAL 12
EL MARQUÉS
01 800 400 2003


IEEQ
CONSEJO DISTRITAL 14
CADEREYTA DE MONTES
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


IEEQ
Instituto Electoral del
Estado de Querétaro
CONSEJO DISTRITAL 15
JALPAN DE SERRA
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


IEEQ
CONSEJO MUNICIPAL
AMEALCO DE BONFIL


IEEQ
Instituto Electoral del
Estado de Querétaro
CONSEJO MUNICIPAL
ARROYO SECO
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


IEEQ
Instituto Electoral del
Estado de Querétaro
CONSEJO MUNICIPAL
COLÓN
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


IEEQ
CONSEJO MUNICIPAL
EZEQUIEL MONTES


IEEQ
CONSEJO MUNICIPAL
HUIMILPAN


IEEQ
Instituto Electoral del
Estado de Querétaro
CONSEJO MUNICIPAL
LANDA DE MATAMOROS
PROCESO ELECTORAL LOCAL 2017 - 2018
www.ieeq.mx
01 800 400 2003


CONSEJO MUNICIPAL
PEÑAMILLER
www.IEEQ.mx
01 800 400 2003


CONSEJO MUNICIPAL
PINAL DE AMOLES
01 800 400 2003


CONSEJO MUNICIPAL
SAN JOAQUÍN
PROCESO ELECTORAL LOCAL 2017 - 2018
www.IEEQ.mx
01 800 400 2003


Instituto Electoral del
Estado de Querétaro
CONSEJO MUNICIPAL
TOLIMÁN
PROCESO ELECTORAL LOCAL 2017 - 2018

- Introducción

Simultáneamente al proceso de revisión de configuración de infraestructura y pruebas de penetración de la infraestructura del PREP, se realizó un escaneo de vulnerabilidades. Una vez identificados los puntos de vulnerabilidad el análisis se enfocó primordialmente en servidores, aplicaciones web, equipos de telecomunicaciones y estaciones de trabajo (estos últimos en el COPREP).

Una vez determinado los activos a analizar se utilizaron además las siguientes herramientas para el pentest: OWASPZAP 2.7, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest. Se realizó ataque desde el interior y el exterior tratando de cambiar los datos en el AEC, los datos de la Base de datos o inutilizar los equipos para que no se pudiera realizar alguno de los procesos del PREP.

- Resultados Generales

Se determinó que los servidores están protegidos adecuadamente.

Las aplicaciones web no pueden modificarse desde fuera de las instalaciones y el personal del PREP no tiene posibilidades de alterar el contenido de las mismas.

Los equipos de telecomunicaciones sólo pueden fallar por desconexión física, pero el Instituto cuenta con, al menos, una conexión de respaldo en cada CATD, la mayor velocidad disponible en la zona. Resistieron los ataques internos de negación de servicio.

Se revisaron las instalaciones del CCV y en las mismas se encontró que, a pesar de los ataques, la estaciones de trabajo de los capturistas y verificadores siguieron trabajando sin problemas. Adicional a esto, se tiene como plan de contingencia el mover a un sitio alterno en caso de una falla total en las instalaciones del Instituto.

Para cada instalación se generó un reporte como el siguiente y se entregaron al instituto aquellos que eran necesario mitigar. Esto se verificó y se aprobó.

PREP 2018 CFATA UNAM
Report generated by Nessus™

CATD-M-Corregidora
Wed, 02 May 2018 12:57:13 CDT

TABLE OF CONTENTS

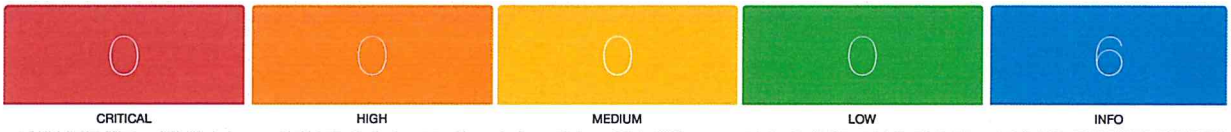
Hosts Executive Summary

Collapse All | Expand All

192.168.1.1

Show Details

192.168.1.10



Show Details

INFORME DE RESULTADOS DE PRUEBA DE NEGACION DE SERVICIO A SITIOS WEB DEL PREP QUERÉTARO

- Introducción

El acceso a los servicios de internet, ha permitido que más personas puedan obtener información para desarrollar ataques en la web. Esto ha generado amenazas entre las que las cibernéticas son un factor importante; por está razón es necesario que los datos contenidos en el PREP tengan una validación de disponibilidad.

La auditoría tiene como objetivo asegurar la correcta y continua disponibilidad del servicio web de los sitios de publicación de resultados del PREP, durante el período de operación.

- Pruebas realizadas

Para los ataques se utilizaron las instalaciones del CFATA y la conexión a internet de la Red Niba.

Se realizaron ataques en la capa de aplicación (HTTP) con diversos escenarios de SLOWLORIS ATACK como son:

a. Slow headers: consiste en enviar las cabeceras HTTP incompletas (sin el CRLF final que indica el final del header) de tal forma que el servidor no considera las sesiones establecidas y las deja abiertas, afectando al número de conexiones máximas configuradas.
b. Range (Apache killer): se crean numerosas peticiones superponiendo rangos de bytes en la cabecera (HTTP ranges), agotando los recursos de memoria y CPU del servidor.
c. Slow read: en este caso se envían peticiones HTTP legítimas, pero se ralentiza el proceso de lectura de la respuesta, retrasando el envío de ACK (HTTP es TCP).

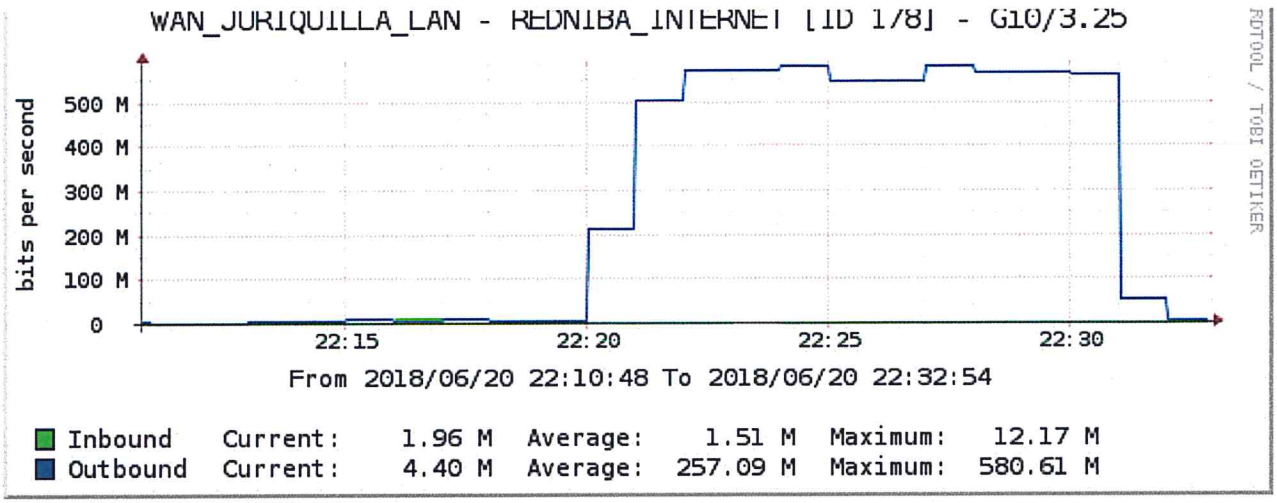
Se realizaron ataques volumétricos por los protocolos TCP (con SYN FLOOD), UDP (con DNS Amplification), ICMP con (ICMP Flood); empleando IP aleatorias, para que no se identificara el atacante. Al mismo tiempo se simuló trafico legítimo.

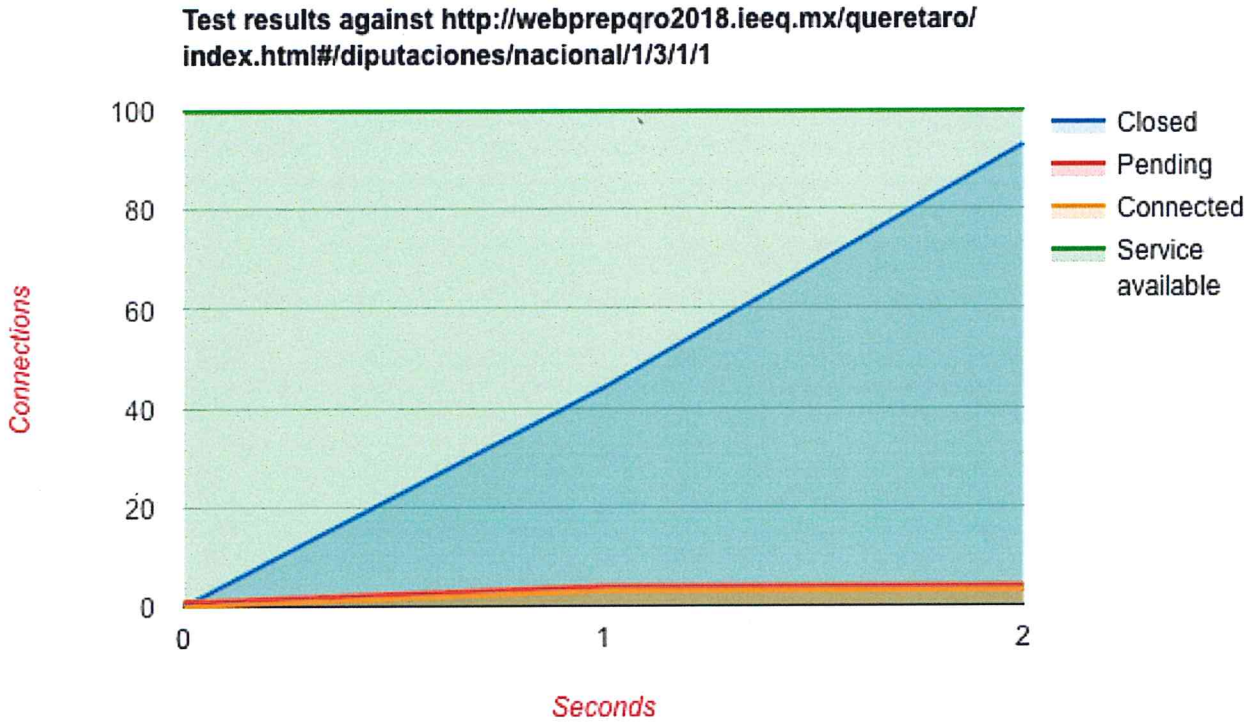
El servidor analizado fue el de webprepqro2018.ieeq.mx y, para el ataque slowloris, se inició con la página /#/Diputaciones/Entidad/Distritos, el cual fue previamente escaneado para obtener sus vulnerabilidades y explotarlas durante el ataque.

- Resultados

1. El escaneo no proporcionó información de vulnerabilidades.
2. El servicio conservó su continuidad ante el ataque de slowloris
3. La página al llegar a los 500M solo uno de los equipos en trafico legitimo tardo 30 segundos en mostrarla pero continuó respondiendo adecuadamente ante el trafico de red, de hasta 580.61M.

Se muestran las gráficas de resultados del ataque volumétrico y un ejemplo del slowloris .





ATENTAMENTE	VOBO
M. EN C. GUILLERMO VÁZQUEZ SÁNCHEZ RESPONSABLE TÉCNICO DE LA AUDITORIA	DR. JOSE LUÍS ARAGÓN VERA DIRECTOR DEL CFATA