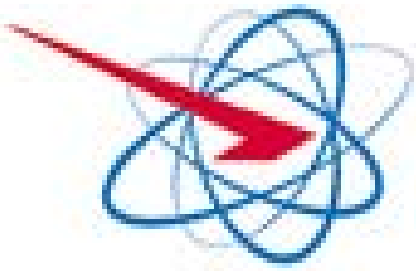


C F A T A

Informe Final

del Programa de Resultados Electorales Preliminares

del Instituto Estatal Electoral de Aguascalientes

2022

3 de junio de 2022

INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO PREP AGUASCALIENTES 2022

- 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 Programa de Resultados Electorales Preliminares (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 Actas de Escrutinio y Cómputo (AEC) sean los que se reflejan en la publicación, Página Web Pública del PREP.

- Metodología

La revisión se realizó en 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 Estatal Electoral de Aguascalientes (IEEAgs) son: acopio, digitalización, foliación, 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, en su última versión.

- Resumen Ejecutivo

Se utilizaron los equipos instalados por la empresa Podernet en los Centros de Acopio y Transmisión de Datos (CATD), y se permitió acceso a los servidores para las pruebas de los módulos de Foliación, Captura y Validación, y de Publicación de Resultados.

Se aplicaron los casos de prueba para cada módulo, que solo para el caso de las urnas electrónicas se realizó el miércoles 11 de mayo, las cuales fueron incluidas antes del primer simulacro.

Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en las oficinas del Centro de Captura y Verificación (CCV), los modulos de Foliación, Captura y Validación.

Las urnas electrónicas se incluyeron adecuadamente durante los simulacros, pero solo hasta el tercero participó personal de INE para su captura.

Se debe considerar que dichas urnas electrónicas requieren de la programación por parte de personal de IEE Jalisco, por lo que cualquier cambio debe incluir este tiempo adicional a los requeridos para la reprogramación del PREP.

- Resultados

El sistema informático permite la captura, digitalización y publicación de los datos asentados en la AEC que se reciben en los CATD.

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, el cual solo incluye la digitalización y transmisión.

El sistema maneja la Integridad en el registro de la información: que a partir de un AEC en papel, se genere una imagen digital completa y legible de ésta y sea almacenada sin alteraciones en su contenido y publicada para consulta; que la imagen digital del AEC, así como sus datos capturados manualmente sean debidamente asociados a la casilla, sección y distrito que corresponda; que los resultados del AEC capturados sean asociados fielmente al partido, coalición o rubro en el cual se registren. Para el caso de los resultados de las urnas electrónicas, el sistema integra directamente el archivo en PDF a la página y los datos son ingresados directamente al PREP.

Para la revisión de desempeño se consideró 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**.

- Resumen ejecutivo

Las pruebas realizadas consistieron 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 y determinar el nivel de exposición de información sensible.

Se evaluó la configuración de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática. Se presento un oficio sobre las urnas electrónicas.

La revisión de configuraciones se enfocó en el sistema operativo de servidores, consolas y dispositivos. 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 obtuvieron, como resultado de la ejecución del pentest y de la revisión de configuraciones, se analizaron y se clasificaron.

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 Podernet 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 determinado lo anterior, se designaron los activos primordiales a revisar, se utilizaron además las siguientes herramientas para el pentest: OWASPZAP, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest.

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

El servicio de pruebas de penetración y análisis de vulnerabilidad para la infraestructura tecnológica, tuvo 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 consistió en la identificación de vulnerabilidad en objetivos específicos, así como en otros que podrían proporcionar acceso a información del PREP,

intentando explotar las vulnerabilidades 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 vulnerabilidades que trataron 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 los objetivos que pueden ser alcanzados 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 ejecutan en las instalaciones de la organización.

- Alcance

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.

Para la revisión de la infraestructura se revisaron las instalaciones de los 18 CATD Distritales, las instalaciones del CCV y su sede alterna, y los servidores en la nube.

- Resultado de la Verificación.

Se atendieron los hallazgos de manera satisfactoria para la infraestructura, en materia de configuraciones de infraestructura y, las pruebas de penetración determinaron que l**a 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.


CENTRO
Contigo


CRENA
VIVA LA


UNIDAD REGIONAL
DE SERVICIOS
EDUCATIVOS
"INSURGENTES"
IEA


CENTRO
Contigo


CENTRO
Contigo
NAZARIO
ORTIZ GARZA


"OJOCALIENTE"
IEA


CENTRO
Contig
GUADALUPE
PERALTA


CENTRO
Contigo
OBRAJE


UNIDAD REGIONAL
DE SERVICIOS
EDUCATIVOS
"SUR"
IEA

- 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 CCV).

Una vez determinado los activos a analizar, se utilizaron además las siguientes herramientas para el pentest: OWASPZAP, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest. Se realizaron ataques 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 la empresa cuenta con, al menos, una conexión de respaldo en cada CATD. 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 todo el personal siguieron trabajando sin problemas.

Para cada instalación se generó un reporte como el que se muestra enseguida y solo se entregaron a la empresa aquellos que eran necesario mitigar. No se presentaron riesgos en los CATD.

Todos los hallazgos fueron atendidos y revisados a mas tardar en el tercer simulacro. Las recomendaciones de buenas practicas se revisaron el 31 de mayo.

XXX.XX.X.108

Crítico	Alto	Medio	Bajo	Información
0	0	4	1	40

Vulnerabilities

15901 - SSL Certificate Expiry -

Synopsis
The remote server's SSL certificate has already expired.

Description
This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution
Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor
Medium

CVSS Base Score
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Plugin Information
Published: 2004/03/12, Modified: 2021/03/02

Plugin Output
The SSL Certificate has already expired:
Subject: C= CN, ST=unknown, L=unknown, O=unknown, CN=XXX.XXX.X.108
Issuer: C= CN, ST=ZheJiang, L=HangZhou, O=DahuaTech, CN=Product Root CA-
Not valid before: Feb 20 10:27:15 2017 GMT
Not valid after: Feb 22 10:27:15 2020 GMT

INFORME DE RESULTADOS DE PRUEBA DE NEGACION DE SERVICIO A SITIOS WEB DEL PREP AGUASCALIENTES 2022

- 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 con la conexión a internet de TotalPlay y Telmex. Fungiendo como testigos el personal de Telecomunicaciones del Campus Juriquilla.

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 no malintencionado con el que se simuló tráfico legitimo.

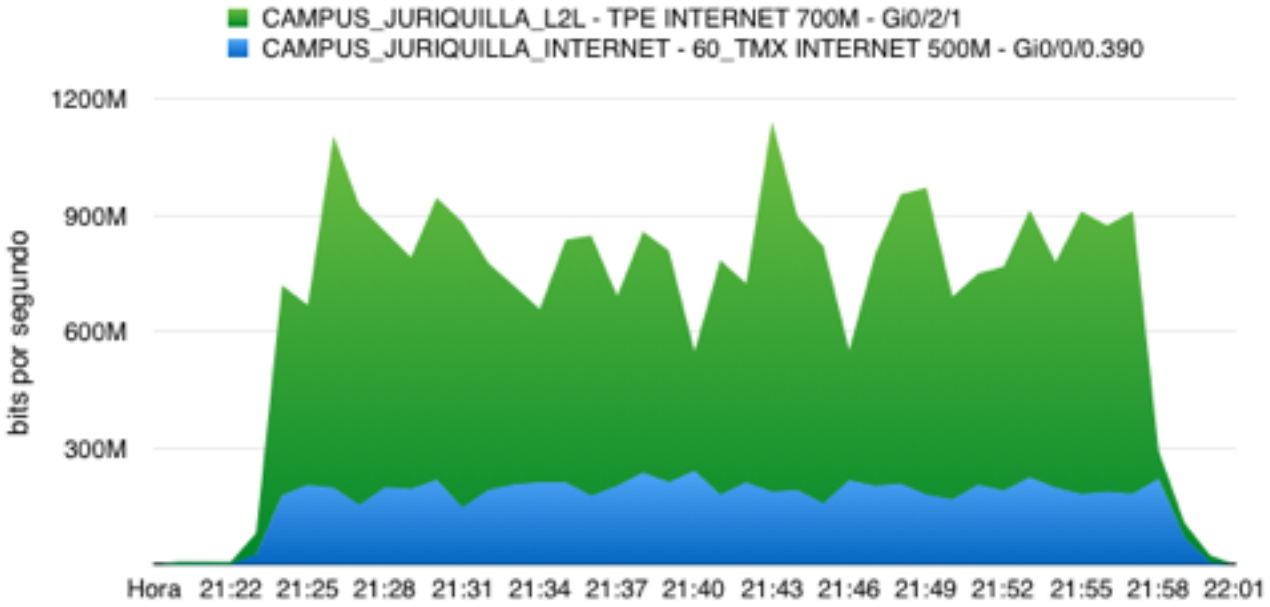
Se analizaron tres veces los servidores testing-725ggs.prep2022-ags-iee.mx y, para el ataque slowloris, se inició con la página /XXADyaeH7zia4ohGh5mu6pooXX/, el cual fue previamente escaneado para obtener sus vulnerabilidades y explotarlas durante el ataque.

- Resultados

1. El escaneo no proporcionó información de vulnerabilidades de alto riesgo.
2. El servicio conservó su continuidad ante el ataque de slowloris, y en algunos casos fueron bloqueadas al detectarse.

3. **La página, al llegar a los** 600M **continuó respondiendo adecuadamente ante el tráfico de red**, se iniciaron nuevos ataques a bases de datos y el servicio continuó funcionando.

Se muestran las gráficas de resultados del ataque volumétrico.



Juriquilla Querétaro a 3 de Junio de 2022

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