

## **Informe de Resultados de las Pruebas de Ataque de Denegación de Servicio (DOS) al sistema Informático del PREP**

Tráfico generado durante las pruebas de denegación de servicio  
(DOS) hechas hacia el sistema informático del PREP del IEE Sinaloa

### **Descripción breve**

Este documento contiene las estadísticas de tráfico generado durante las pruebas de un ataque de negación de servicio (DOS) como parte de la auditoría de seguridad del PREP

Roberto Luis Iriarte / Raime Alejandro Bustos

roberto@iriarte.net

raime.bustos@tec.mx

Jesús R. González / Juan Arturo Nolasco

jrgonza@gmail.com

jnolasco@itesm.mx

### Índice

1	Introducción	2
2	Objetivo	2
3	Alcance	2
4	Pruebas que aplicar	2
4.1	Ataque volumétrico por TCP - SYN FLOOD	3
4.2	Ataque volumétrico por UDP - DNS AMPLIFICATION	3
4.3	Ataque volumétrico por ICMP - ICMP FLOOD	4
4.4	Ataque en la capa de aplicación – SLOWRIS ATTACK	4
4.5	Controles complementarios o compensatorios	5
5	Observaciones en las pruebas y recomendaciones	6

Versión	Fecha	Descripción
1.0		Documento base para tomar resultados y las estadísticas de tráfico generadas durante el ataque de negación de servicio a la infraestructura del PREP
1.1	14/Abr/2021	Cambio de formato de documentación

Dictamen elaborado por:

MSc. Jesús Raúl González Hernández en coordinación con el Dr. Juan Arturo Nolasco, Ing. Roberto Luis Iriarte Pablos y MSE Raime Alejandro Bustos Gardea.

### 1 Introducción

Este documento pretende documentar los resultados de las pruebas de los ataques de DOS realizadas como parte del cumplimiento del anexo técnico de los servicios de auditoría del sistema informático y la infraestructura tecnológica del PREP del **IEE Sinaloa** para la jornada de elecciones del 2021.

### 2 Objetivo

El objetivo de estas pruebas es para validar la resiliencia y funcionamiento de la plataforma informática bajo un ataque de tráfico en varios escenarios que afecten el funcionamiento de esta.

### 3 Alcance

El alcance de las pruebas se restringe al centro de procesamiento del **IEE Sinaloa** siendo la plataforma del PREP la que se pretende medir con este tipo de afectación. La plataforma de procesamiento se encuentra hosteada en IBM Cloud.

### 4 Pruebas que aplicar

Las pruebas que se está solicitando como parte del ejercicio de auditoría del PREP como parte del anexo técnico del INE en cuanto a negación de servicio son:

<ul style="list-style-type: none"><li>• Ataque volumétrico por protocolo TCP donde se requiere lo siguiente: Al menos 400 Mbps de capacidad total contra el sitio central Realizar un SYN FLOOD hacia el sistema</li><li>• Atque volumétrico por protocolo UDP Al menos 400 Mbps de capacidad total contra el sitio central</li></ul>	<ul style="list-style-type: none"><li>• Ataque volumétrico por protocol ICMP Al menos 400 Mbps de capacidad total contra el sitio central Realizar un ICMP FLOOD hacia el sistema</li><li>• Ataque en la capa de aplicación Realizar un ataque del tipo SLOWRIS ATTACK</li></ul>
---	--

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>Realizar un ataque del tipo DNS AMPLIFICATION</li> </ul> | <ul style="list-style-type: none"> <li>Controles compensatorios en caso que las pruebas no se puedan llevar a cabo</li> </ul> |
|---|---|

#### 4.1 Ataque volumétrico por TCP - SYN FLOOD

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Sinaloa 2021				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPN01 – La infraestructura debe soportar un ataque volumétrico TCP-SYN FLOOD	Se realizará una inundación de tráfico al sitio de publicación mediante el uso de hping: root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source <Sitio_Prueba>	Se documentará el nivel de tráfico y el desempeño del servidor bajo esta situación	Cloudflare con su red global de 67 Tbps es capaz de mitigar cualquier ataque volumétrico TCP-SYN FLOOD  <a href="https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/">https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/</a>	Sustituída

#### 4.2 Ataque volumétrico por UDP - DNS AMPLIFICATION

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Sinaloa 2021				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS Amplification.	Para evitar afectación al proveedor desde donde se origina el ataque hará una revisión de los DNS públicos del siguiente modo: 1. Se consultará el sitio <a href="https://openresolver.com">https://openresolver.com</a>  Se escaneará el DNS para verificar que la recursividad está habilitada Usando el software NMAP para hacer el escaneo al DNS mediante el comando:	En cualquiera de los dos casos, el resultado deberá ser que la recursividad está habilitada en el DNS	Se revisó el DNS que está ubicado en Cloudflare para revisar si estaba habilitada la recursividad, se encontró que no está habilitado	Aceptado

	<pre>nmap -sU -p 53 -sV -P0 --script "dns-recursion" x.x.x.x &lt;x.x.x.x siendo la dirección del servidor de DNS&gt;. Esto deberá arrojar un resultado similar al siguiente: PORT STATE SERVICE VERSION 53/udp open domain ISC BIND "version" * _dns-recursion: Recursion appears to be enabled*</pre>			
--	--	--	--	--

### 4.3 Ataque volumétrico por ICMP - ICMP FLOOD

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Sinaloa 2021				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPN03 – LA infraestructura deberá poder soportar un ataque volumétrico por ICMP – ICMP FLOOD	<p>El ataque se hace utilizando el comando hping3 seleccionando la opción de flood</p> <pre>root@kali:~# hping3 --flood --rand-source --icmp -p 80 (direccion_IP)</pre>	Se documentará el nivel de tráfico recibido para verificar que el servidor ha sido inundado de paquetes desde la dirección origen	<p>Cloudflare con su red global de 67 Tbps es capaz de mitigar cualquier ataque volumétrico ICMP FLOOD</p> <p><a href="https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/">https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/</a></p>	Sustituída

#### 4.4 Ataque en la capa de aplicación – SLOWRIS ATTACK

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Sinaloa 2021				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación vía un SLOWLORIS attack	<p>se hará con la herramienta <b>slowhttptest</b> la cual se puede configurar para generar este tipo de conexiones incompletas</p> <pre>root@kali:~# slowhttptest -c 1000 -H -g -o Trafico_slowloris -i 10 -r 200 -t GET -u http://sitio.remoto.mx -x 24 -p 3</pre>	Se documentará la respuesta y desempeño del servidor con este tipo de ataques.	<p>Cloudflare con su red global de 67 Tbps es capaz de mitigar cualquier ataque tipo SLOWLORIS.. Todas las peticiones que recibe las pone en un buffer por lo que, en resultado, nunca llegan al origen, los servidores del OPL.</p> <p><a href="https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/">https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/</a></p>	Sustituída

### 4.5 Controles complementarios o compensatorios

Los siguientes pruebas son para revisar controles complementarios o compensatorios, dependiendo de la situación sobre la factibilidad de hacer ataque o no (dada la ubicación de los recursos a probar)

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Sinaloa 2021				
Prueba	Pruebas ejecutadas o descripción	Criterio de Aceptación	Comentarios	Resultado
<b>SPN05</b> – Validación de las cuotas de servicio configuradas en las suscripciones de servicios de nube (si aplica)	Se entrará a la consola bajo la suscripción de la OPL y verificará que haya una cuota de tráfico definida para propósitos de limitación de este a los servidores definidos	Se verificará dichas cuotas de tráfico las cuales deberán ser apropiadas con el ancho de banda designado para el sitio de publicación.	El esquema de protección de Cloudflare para DOS/DDOS solo permite configuración básica y estándar y no permite configuración de cuotas de tráfico.  <a href="https://www.cloudflare.com/ddos/">https://www.cloudflare.com/ddos/</a>	<b>Sustituída</b>
<b>SPN06</b> – Revisar con la OPL la existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS	Verificar con el encargado de informática de la OPL que exista un manual de procedimiento a seguir en caso de un evento de ataque de negación de servicio.	La OPL deberá mostrar un procedimiento a seguir interno o hacia el proveedor que tengan con estos servicios de protección de DOS	Se encuentra el procedimiento dentro del <i>Plan de Seguridad Continuidad y Análisis de Riesgos</i>	<b>Aceptado</b>
<b>SPN07</b> - Validar la existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS	Verificar con los encargados de la OPL que existan contratos y/o servicios que ofrezcan protección contra ataques de DOS	La OPL deberá de mostrar evidencias de servicios de protección contra ataques de negación de servicio	Se cuenta contratado el servicio de protección DDoS por parte de Cloudflare	<b>Aceptado</b>
<b>SPN08</b> – Validar la existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS	Revisar con la OPL que exista un plan definido de comunicación hacia la comunidad que el área de comunicación pueda dar en caso que se presenten este tipo de incidentes.	Plan debe existir y debe estar validado tanto por el área de tecnología de la OPL como por el área de comunicación y con el visto bueno del Consejero Presidente de la OPL	Incluido en el <i>Plan de Seguridad Continuidad y Análisis de Riesgos</i>	<b>Aceptado</b>

### 5 Observaciones en las pruebas y recomendaciones

Las observaciones y recomendaciones se harán sobre el anexo correspondiente de pruebas que se esté realizando y bajo los criterios que se detallan por cada una de ellas. En esta sección se presenta un resumen, en función de los resultados y revisión de hallazgos, de los resultados de esta y su cumplimiento, así como hallazgos por clasificación que se de.

Los criterios que se usaron para la ejecución y presentar el resumen se describen en la siguiente tabla los cuales son usados en todas las tablas subsecuentes.

Definición	Descripción	Acciones
<b>Aceptado</b>	La prueba cumplió satisfactoriamente con los criterios de aceptación	Prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
<b>Rechazado</b>	La prueba no cumplió con los criterios de aceptación	La prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
<b>Aceptado con Observaciones</b>	La prueba cumplió con una parte de los criterios no cumplió totalmente con observaciones.	Prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no serían obligatoria su implementación y solo queda como sugerencia o recomendación.
<b>No Ejecutada</b>	Prueba no fue ejecutada en el ciclo por cuestiones de tiempo o por decisión mutua	La prueba se volverá a ejecutar en otro ensayo o bien si no se ejecuta, se agregará la justificación del por qué de esto.
<b>Sustituida</b>	Prueba inicialmente diseñada pero que se intercambio por otra acción debido a cierta condición de la prueba inicial	La prueba que inicialmente se planeó no fue ejecutada dado que alguna condición de esta se debía modificar, cambiar o modificar al momento de su ejecución