ESTRATEGIA COGNITIVA PARA LA EVALUACIÓN DE UNA CENTRAL IP BASADA EN ASTERISK FRENTE A LOS ATAQUES DoS

COGNITIVE STRATEGY FOR EVALUATING AN IP CENTER BASED ON ASTERISK FACED DoS ATTACK

Guijarro Rodríguez Alfonso[1] (alfonso.guijarror@ug.edu.ec)

Cevallos Torres Lorenzo[2] (lorenzo.cevallost@ug.edu.ec)

Torres Villegas Ignacia [3] (lorenzo.cevallost@ug.edu.ec)

RESUMEN

El manejo de políticas de seguridad es primordial para cualquier compañía o institución, ya que depende de estos criterios que su información, permanezca almacenada de forma segura y confiable, en la actualidad contamos con dispositivos de seguridad como: firewall, detectores de intrusos, entre otros. Se ejecutan auditorías internas y externas con la finalidad de verificar los niveles de seguridad perimetral de una empresa y detectar la posible fuga de información por parte de los funcionarios. Dado este antecedente, en el proyecto se realiza una evaluación sobre el comportamiento de una Central Telefónica Elastix, mientras recibe un ataque basado en Denegación de Servicio, con el cual se demuestra el comportamiento a nivel de servicio, ancho de banda y red en general, para esto se diseñó un escenario de prueba, el cual permitió registrar una bitácora de eventos y comportamiento para elaborar un sistema de contingencia que logre mitigar los ataques.

PALABRAS CLAVES: Ataques informáticos, centrales telefónicas, elastix, sistemas detectores de intrusos, seguridad informática, seguridad perimetral.

ABSTRACT

Management of security policies is essential for any company or institution, as it depends on the criteria for their information, such as users is stored safely and reliably, today we not only have safety devices, such as firewalls, intrusion detectors, but with both internal and external audits to verify a company's perimeter security and data leakage by their officials. With this information, my project investigates the assessment of the behavior of a Call Center Elastix as it receives a computer attack, showing what happens to both your service, bandwidth, and the network in general, allowing us to create a blog events and situations to form our system of these unforeseen contingency.

---

[1] Ingeniero en Computación en la Escuela Superior Politécnica del Litoral. Máster en Modelado Computacional en Ingeniería. Universidad de Cádiz. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales. Universidad de Guayaquil.

[2] Ingeniero en Estadística Informática. Escuela Superior Politécnica del Litoral. Máster en Modelado Computacional en Ingeniería. Universidad de Cádiz. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales. Universidad de Guayaquil.

[3] Ingeniera Civil. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería Civil. Máster en docencia Universitaria.

KEY WORDS: cyberattacks, elastix, informatic security, intrusion detection system, perimeter security, telephone exchanges.

La telefonía IP ha logrado una evolución sin precedentes entorno al mundo de las comunicaciones y la informática, por lo cual es difícil imaginar que alguna entidad comercial no cuente con una comunicación telefónica, dado que este es un medio de primera necesidad entre las empresas y el mundo exterior. Sin embargo, es el objetivo principal de agentes maliciosos, motivo por el que se pretende evaluar el comportamiento y la seguridad de una central telefónica IP, frente a los delitos informáticos objeto de este estudio, como los ataques por denegación de servicio (Denial Of Services), conocido normalmente como Ataques DoS por sus siglas en inglés.

Varios autores han desarrollado temas relacionados a la seguridad informática y sus técnicas de contingencias. Landívar (2008) conceptualiza la telefonía IP e introduce a los lectores al campo de las centrales telefónicas elastix; Álvarez y Yépez (2011), recrean ambientes reales para comunicar dos centrales elastix de distintos colegios; Santos (2008) profundiza en el tema de las centrales telefónicas y propone una comparativa entre una central telefónica convencional frente a una con una computadora con software elastix; Christian (2013) realiza la implementación de una central telefónica en la nube al constatar y verificar las ventajas y desventajas frente a una instalación local; (Sotomayor, 2013) ejecuta escenarios de prueba para analizar las vulnerabilidades de las centrales elastix en IPV4; por último, Cáceres (2014) analiza las vulnerabilidades telefónicas en centrales elastix que funcionan con IPV6.

Para el desarrollo de esta investigación, se propone evaluar el rendimiento operacional y técnico en las centrales telefónicas IP, y se realizan varios ataques de los que son susceptibles, con lo cual, se identificaron las herramientas usadas por los atacantes, los tipos de amenazas de seguridad y se evidenciaron las vulnerabilidades que se presentan, lo que permitió definir las medidas de contingencia, cabe mencionar que esta práctica se realizó en un ambiente laboral dentro del Instituto de Normalización, donde se maneja un total de 19 extensiones por todos los departamentos en la ciudad de Guayaquil.

Esta investigación está basada en un estudio de campo de las centrales IP, así como en una revisión bibliográfica; el primero permitió observar el comportamiento de las centrales IP, su funcionamiento y sus vulnerabilidades para evaluar la seguridad de las mismas. El segundo ayuda a relacionar eventos pasados en base a estudios realizados por autores especializados en el área.

En el proyecto se realiza una investigación explorativa-experimental, cuyo propósito es evaluar el comportamiento de las centrales IP bajo el ataque DoS, con el propósito de implementar la seguridad y encontrar soluciones que permitan facilitar y mejorar la comunicación entre usuarios.

Para poder obtener información sobre los puertos habilitados y las diferentes vulnerabilidades que se tienen, se realiza un escaneo de puertos en la central IP, en el cual se encontraron brechas abiertas a ataques externos.

La información obtenida por medio del escaneo de puertos, sirve como medio para probar las hipótesis, y alcanzar los objetivos de la investigación. Por lo cual, los

datos deben ser pertinentes, confiables para lograr definir las técnicas y fuentes de recolección.

Es una aplicación desarrollada como software libre, que implementa una central telefónica (PBX), basado en las licencias públicas (GNU/Linux), lo que permite su descarga desde cualquier sitio web. Este modelo de central como cualquier PBX, se le pueden conectar un número determinado de teléfonos IP, según los recursos físicos que preste el equipo, lo cual permite la comunicación directa entre ellos y más aún, permite el VoIP.

Esta central en específico, incluye un número de características principalmente para los sistemas propietarios de los PBX, los cuales son: Distribución automática de llamadas, IVR, conferencias, buzón de voz, conferencias, colas, entre otras características.

Este modelo de central viene con la compatibilidad de algunos sistemas operativos, lo que le permite no solo la conexión con sistemas Linux, sino también con otros sistemas operativos, pero Linux siempre es el principal, pues da una gran apertura a un sin número de servidores, capaces de poder soportar el software y la transmisión del servicio de un host a otro.

Dentro de sus accesorios es importante mencionar que para poder conectarse a las redes de telefonía convencional, es necesario adaptarles las tarjetas electrónicas con puertos FXS, FXO, T1, E1, entre otras más, lo que permite, así no solo la comunicación entre usuarios, sino el servicio de calidad brindado por el mismo.

Según Salcedo, López y Hernández (2011) una de las ventajas principales de Asterisk es su licenciamiento gratuito, puesto que ofrece la oportunidad de brindar servicios que mantienen costos muy elevados, y hacen más sencilla y accesible la utilización de los mismos, servicios tales como: IVR, buzón de voz, protocolos SIP, entre otros.

- **Protocolos**

Como parte de los protocolos se encuentra el protocolo VoIP, que es un lenguaje que permite el transporte de las conversaciones telefónicas sobre redes IP en tiempo real, transportándolas en paquetes IP. Dentro de las comunicaciones VoIP, se pueden diferenciar dos grupos de protocolos, que tienen definidos sus funciones, las cuales son:

- Transporte y Control: son los protocolos tradicionales de las redes IP, TCP/ IP/ UDP/ RTCP/ RTP.
- Señalización: son los protocolos que se han desarrollado a medida que se requieren o crece el servicio. Estos protocolos se pueden subdividir a su vez en: propietarios (Skype, Cisco) y Código Abierto (H.323, IAX).

Técnicas de ataques

- Denegación de Servicio

Su objetivo principal es impedir el acceso a los sistemas y recursos de los servicios durante un lapso indefinido de tiempo, ya que estos ataques son realizados en su mayoría a los servidores de grandes empresas. Sus acciones no

son las de recuperar o alterar algún tipo de información, sino más bien el de destruir la reputación de las mismas en impedir sus procesos, por lo cual se asume que estos tienen relación con procesos informáticos.

Estos tipos de ataques se dividen en dos partes:

- Denegación de servicio por saturación.
- Denegación de servicio por explotación de vulnerabilidades.

Cuando este tipo de ataques es realizado por varios equipos, es conocido como “Denegación de Servicio Distribuido” (Distributed Denial of Service), y se realizan diferentes tipos de ataques, desde diferentes equipos a la misma granja de servidores, lo que provoca la explotación de las vulnerabilidades, la saturación de la red y colapso del servicio.

Dentro de los ataques por DoS se encuentra:

- Fuerza Bruta

Este tipo de ataque se caracteriza por una incansable secuencia de ataques, con el único fin de obtener algún usuario y contraseña para poder acceder al sistema (smtp, ssh, http). Para poder efectuar este tipo de ataques, se utilizan programas que comprueben una serie de combinaciones de caracteres o palabras, hasta dar con la correcta, por ello se recurre a un masivo uso de recursos para lograr su cometido.

- Inundación SYN (SYN Flood)

Este ataque procede cuando una máquina se comunica a través del protocolo TCP/IP con otra, enviándole una serie de peticiones junto a la petición real, en su mayoría con direcciones de origen falsificadas, lo cual provoca que el servidor contesta cada una de las peticiones y establece una conexión para responder los paquetes, y espera uno de respuesta, sin embargo, esta respuesta nunca llega porque su dirección de origen es falsa.

- Inundación ICMP (ICMP Flood)

Bajo esta técnica se pretende agotar el ancho de banda de la víctima, enviando de manera continua un sin número de paquetes ICMP de un gran tamaño (ping), lo cual provoca una respuesta (pong) continua y desmesurada y sobrecarga tanto la red como el sistema del usuario.

- Smurf

Es una variante del ataque ICMP Flood, ya que a diferencia del otro este tiene ampliado su efecto, ya que no solo envía paquetes ICMP, sino también los envía a una dirección de broadcast, entregándole en su cabecera la dirección de origen de la víctima (spoofing), lo que obliga a que todos respondan a esa dirección saturando los sistemas de la víctima.

Para realizar la investigación, se recrearon escenarios de prueba, a través del uso de máquinas virtuales para obtener la información necesaria y así evaluar el comportamiento de la central IP Elastix.

Los pasos a seguir en el procedimiento de la investigación son los siguientes:

- Escaneo de puertos en la central IP.
- Presentación de las vulnerabilidades encontradas.
- Ejecución de pruebas de laboratorio para explotar las vulnerabilidades.
- Elaboración del informe de resultados.
- Realizar las conclusiones y recomendaciones.

Un aspecto con gran importancia dentro del proceso de investigación es la obtención de información, ya que de esto dependerá el nivel de confiabilidad y validez de los resultados, la cual es conocida además como trabajo de campo.

Escaneo de puertos en la central IP

Antes de iniciar el ataque DoS, se realizará un escaneo de puertos de la central Elastix, usando Zenmap, la sintaxis que se usara es nmap –T4, el cual es un temporizador, -A para realizar un ack scan y –v para obtener un informe detallado del escaneo, como se observa en la **Figura 1**, el servidor tiene abierto 12 puertos y se pueden ver, las versiones de los servicios que se ejecutan en ellos.

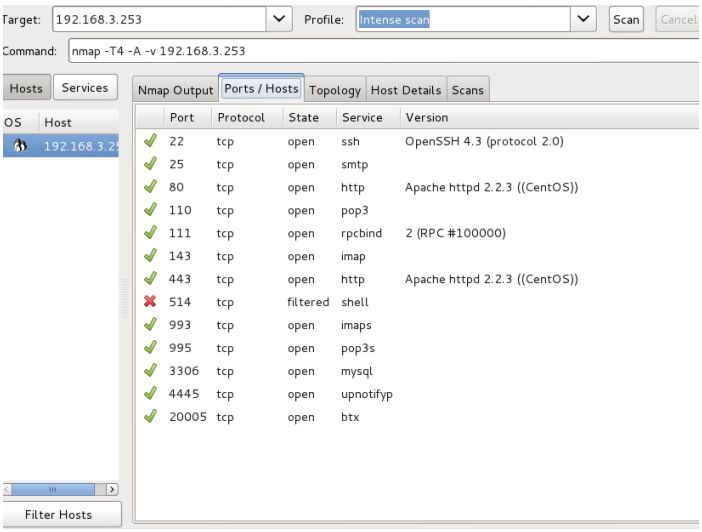

Figura 1: Escaneo de puertos de la central Elastix

Nota: En la **Figura 1** se observa a detalle lo que fue encontrado en el escaneo de la central Elastix, de forma más amigable para el usuario, se observa la versión del Sistema Operativo y la versión del Kernel que posee.

Presentación de las vulnerabilidades encontradas

Como se observa, se ha detallado las principales vulnerabilidades que sufre la central telefónica Elastix, junto con la posible solución tomada como prevención, antes que se suscite el ataque de DoS.

Tabla 1

Vulnerabilidades y Soluciones de Elastix

Vulnerabilidad	**Solución**
Puertos abiertos innecesariamente	Cerrar puertos innecesarios

Enumeración de dispositivos SIP habilitada	Configuración de reglas de acceso en el FW
Permisos de escaneo de usuarios habilitada	Se debe corregir el valor por defecto en el archivo sip. Conf
Robo de contraseñas de usuarios por ataque de fuerza bruta permitido	Se debe corregir el valor por defecto en el archivo sip. Conf
Contraseñas de usuarios inseguras, débiles e intuitivas	Se debe implementar normas y estándares para la creación de contraseñas más robustas
Uso del protocolo SSH sin ninguna protección	Configuración de herramientas de protección, o creación de IP Tables
Contraseña de Súper Usuario (ROOT) débil	Implementar normas y estándares para la creación de contraseñas más robustas
Permiso de solicitudes concurrentes de forma ilimitada	Creación de Ip Tables
Servicios sin usar habilitados	Deshabilitar los servicios que no estén siendo usados

Nota: Fuente:http://repositorio.espe.edu.ec/bitstream/21000/9558/1/AC-RED-ESPE-048527.pdf

Elaborado por: Ing. Carlos Romero, Ing. Fabián Sáenz, Ing. Julio Sotomayor.

Como medidas de prevención en los ISP, se debe tener en cuenta las siguientes:

- Permitir el paso de paquetes que provengan de IPs autorizadas.
- Se debe restringir el número de paquetes TCP/SYN, para evitar el TCP/SYN Flood.
- La plataforma Elastix, cuenta con un módulo de seguridad, el cual incluye un firewall, por defecto no está habilitado, si se configura y habilita correctamente se evitará los accesos no autorizados, su principal funcionalidad es controlar los puertos y servicios que se encuentren en funcionamiento.
- Para evitar los ataques como TCP/DYN Flood y UDP Flood, se puede crear reglas de Ip table, como se muestra en la **Tabla 3**, en donde se detallan las ip tables para evitar estos ataques.

Ejecución de pruebas de laboratorio para explotar las vulnerabilidades

Escenario #1

Para este escenario, usamos Kali Linux, con una IP local para poder tener libre acceso a la Central IP, se utilizó la herramienta Siege, la cual es una prueba de carga de sitios web, fue diseñado con el propósito de evaluar el rendimiento de

servidores Web bajo coacción, como se ve en la **Figura 2**, se abre un terminal y se escribe el comando siege –C350, el cual es el número de conexiones que se va a simular, –t, el tiempo de ejecución del ataque y d1, es el retardo en segundo y, al final, se escribe la IP del objetivo, ya que esta dentro de la red LAN, y se escribe la IP privada**.**

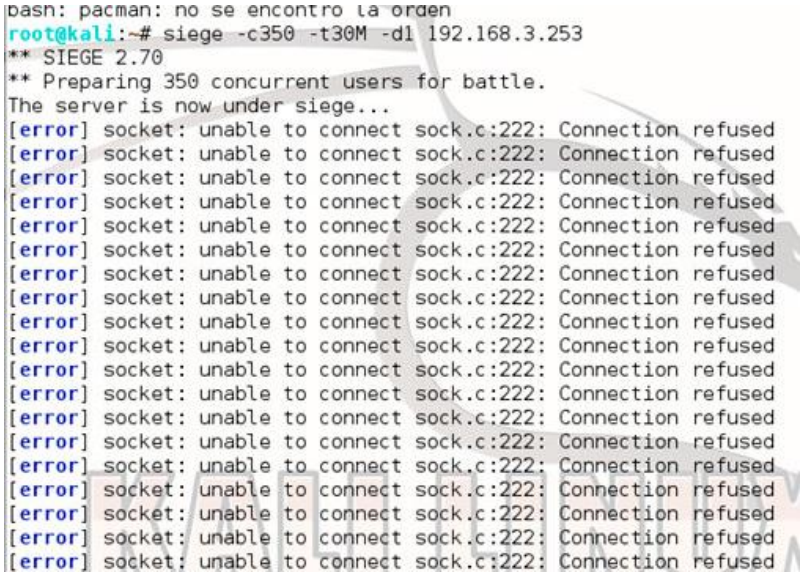

Figura 21: Uso de la herramienta Siege

Una vez iniciado el ataque, intentará conectarse las veces que se desea hacia el servidor Web, por medio de sockets, una vez que establezca las conexiones o peticiones, el servidor no dará ninguna respuesta tal como se observa en la **Figura 3**, donde se encuentra el mensaje “socket: Conection time out”.

Figura 32: Conexiones masivas con siege

Durante el ataque, se consultó en un cliente, el acceso Web hacia la central Elastix, pero debido al número de peticiones que tenía, el servidor no respondió, al detener el ataque, el servidor volvió a funcionar adecuadamente luego de 3

minutos, lo que comprueba la efectividad del ataque, si la central no cuenta con seguridad (**Figura 4**).

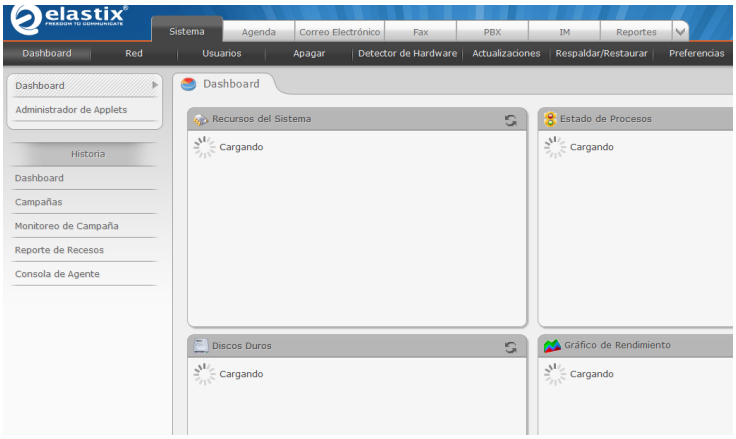

Figura 3: Caída del Servidor Elastix

Durante el ataque, se usó Wireshark para capturar los paquetes que se enviaban a través de la red, donde se notó que, existen un sin número de paquetes ack, como muestra la **Figura 5**, se observa que la central recibe constantemente paquetes TCP retransmitidos, lo que provoca la lentitud en su respuesta.

Figura 54: Captura de paquetes con Wireshark

Escenario #2

En este escenario, se usó Kali Linux, con una IP local dentro de la red LAN, junto con la herramienta SYNFLOOD, el cual permite enviar paquetes SYN al destino, lo cual provoca que el servidor trate de establecer una conexión con el supuesto cliente. Como se estima en la **Figura 6**, se apertura un terminal y se digita el comando msfconsole para usar Metasploit, una vez abierto, se escribe use auxiliary/dos/tcp/synflood, esta herramienta permitirá hacer el ataque de SYNFLOOD.

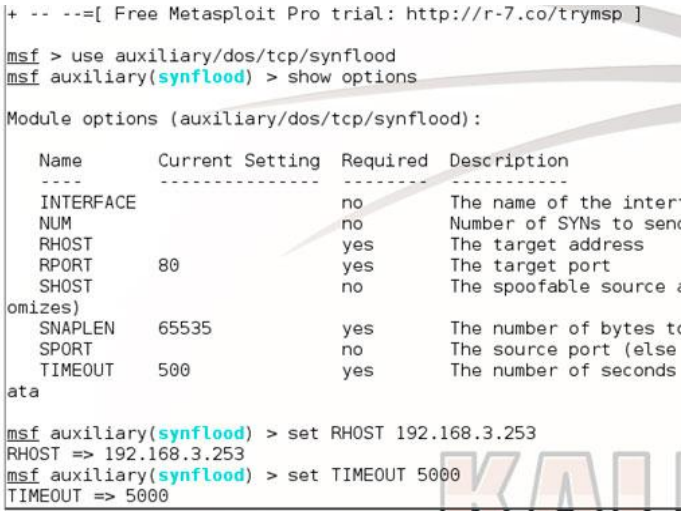

Figura 6: Uso de la herramienta SYNFLOOD

Dentro de la herramienta synflood, se escribe set RHOST, y se digita la IP de nuestra víctima, luego se establece el comando set TIMEOUT y se escribe 5000, para ejecutar el ataque, luego se escribe Run, tal como se aprecia en la Figura 7, se ve que los paquetes de SYNFLOOD, son enviados a la víctima por el puerto 80.

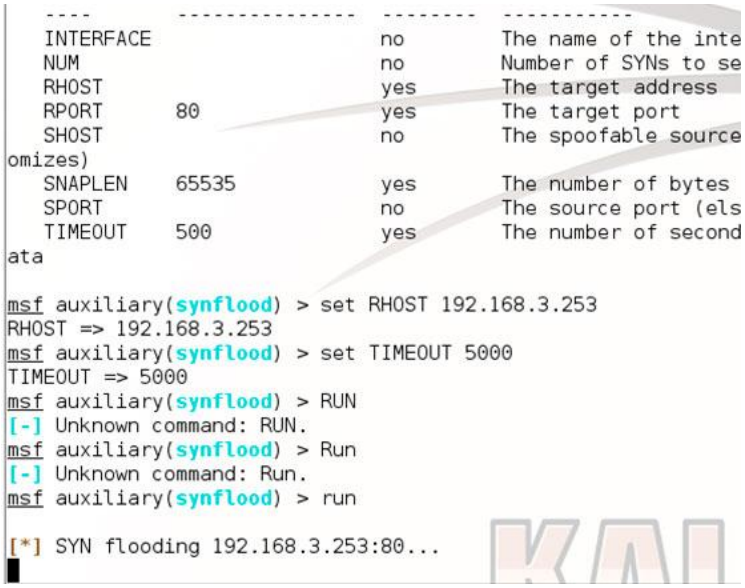

Figura 75: Ejecución de SYNFLOOD

Durante el ataque, se consulta mediante el explorador la central Elastix, pero la central no da una respuesta exitosa, como se muestra en la **Figura 8**, no existe comunicación entre la central y el cliente.

Figura 8: Caída del servidor Elastix

Con la herramienta Wireshark, se capturan los paquetes que se envían y se reciben dentro de la red, y se lo observa en la **Figura 9** que los paquetes que son enviados son TCP todos desde una misma IP hacia la central Elastix, lo que provoca que la central tenga demasiadas peticiones de conexión.

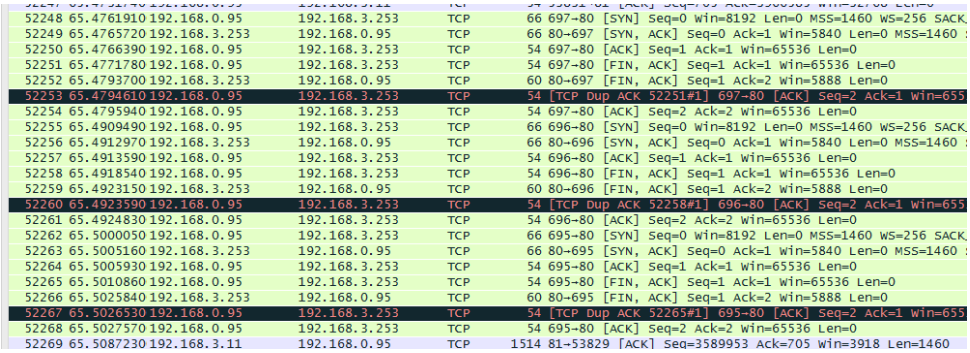

Figura 96: Captura de paquetes con Wireshark

Una vez que se ha monitoreado el estado de los servicios activos, como lo es el almacenamiento en los discos duros, el rendimiento de la memoria física, la saturación de la red y demás procesos propios del sistema, se observó que no existen normas de seguridad, no existe ningún dispositivo de seguridad perimetral, no hay control del uso de los recursos informáticos de la institución.

Además, luego de hacer un escaneo de IP en la red, se comprobó que no hay una segmentación de la red, lo cual provoca que cualquier intruso, entre fácilmente a la red, e incluso, tenga acceso a los servidores.

Para evaluar el rendimiento de la red se usó Wireshark, el cual capturó todos los paquetes que se enviaban y recibían a través de la red, mientras se realizó un MAC Flooding, donde se provocó que el comportamiento del switch se vea afectado, lo que inició un envío masivo de tramas por todos los puertos del switch, es decir el switch se comporta como un hub, que incurre a que nuestra red se degrade poco a poco.

Luego de que se realizó la evaluación del rendimiento, se aplicó una prueba con un medidor de velocidad, para registrar cuales fueron las consecuencias del ataque, se observó que el ancho de banda si se vio afectado, lo que provocó una latencia de 180ms y un decadencia del 3.55 % del ancho de banda, cuya

degradación fue creciendo hasta perder el servicio, el cual fue sentido por todos los usuarios de la institución, quienes vieron su trabajo afectado, al usar los sistemas en línea. (Ver la ilustración 17 y 18)

La central telefónica Elastix, ubicada en el centro de cómputo de la institución, fue el instrumento que se utilizó para el segundo escenario, el cual se basó en realizar un ataque DoS, el cual permitió observar diversas vulnerabilidades que tiene nuestra central, entre ellas: la central no posee ningún dispositivo de seguridad perimetral especializado para centrales telefónicas, por lo cual se tiene libre acceso a la misma; no cumple con las políticas para establecer una contraseña de seguridad, la cual puede ser descifrada por un ataque de diccionario; su dirección IP se encuentra en la vlan de usuarios, lo que permite que cualquier usuario que esté conectado a la misma subred, tenga acceso a nuestra central.

Luego de que se observó la falta de seguridad en la central telefónica por los diferentes escenarios planteados, se realizó un registro de contramedidas de ataques, las cuales se incluyeron en la bitácora, por lo que se crearon y se levantaron reglas de IP table como contramedidas por los mismos.

Luego de haber monitoreado los sistemas activos dentro de la institución, se concluye que es necesario implementar normas de seguridad, ya sea, según Rivera y Poma (2013), una puerta bajo biométrico o huella dactilar, como también la instalación y correcta configuración de un firewall como seguridad perimetral e interna, así mismo un control sobre el ancho de banda usado por cada uno de los usuarios con una debida segmentación de la red para evitar intrusos internos a nuestra central.

Una vez realizado el primer escenario con MAC Flooding se concluye que, teniendo total acceso a la red, sin un firewall como dispositivo de seguridad, filtro o IP table, es muy sencillo degradar el sistema de red poco a poco, hasta que finalmente los usuarios de los sistemas en línea o recursos de red, se vean totalmente paralizados en sus labores, ya que perderán conectividad con los servidores o tendrán un gran retardo en sus respuestas.

Luego de realizadas las pruebas y medir la degradación del ancho de banda, se concluye que el aumento de latencia o retardo en las respuestas, así como el consumo excesivo del ancho de banda se puede percibir con la observación directa de la lentitud de respuesta, también, la pérdida de conectividad con los servidores o recursos del sistema.

Una vez realizada las diferentes pruebas a la central telefónica Elastix, se concluye que está totalmente expuesta a intrusos, ya sea interno o externo, porque al no tener un firewall especializado en centrales telefónicas, ni una segmentación de red, ni política de seguridad en contraseñas, es totalmente factible que con un simple ataque de diccionario, alguien trate de vulnerar el sistema, más aun si no hay un control en la red wi-fi que se encuentra en el mismo segmento de red.

Una vez realizada la bitácora de contramedidas de ataques se concluye que es necesario tener registrado tanto los eventos como los accesos a nuestra central telefónica, ya que, si en el futuro se tiene otra eventualidad similar, se debe tener

la iniciativa de contrarrestar esa situación y por lo menos para el ataque, ya que en su defecto lo correcto sería que este no ocurriera.

Es por estas causas que en la investigación se recomienda:

- Implementar políticas de seguridad tanto para la seguridad física de los equipos, como para la administración de los mismos; adquirir un firewall acorde a las necesidades del administrador y los servicios ofrecidos a los usuarios, así mismo se debe segmentar la red y si es posible dejar creadas y asignadas las vlans para mayor seguridad de los servicios y la información.
- Implementar un sistema de prevención de intrusos, el cual se encargará de controlar los accesos no autorizados a nuestra red o servidores, dando así una alerta en este tipo de eventos, ya que con la activación de sus sensores virtuales, indicará no solo la presencia de ataques, si no también, la de las falsas alarmas; pero este tipo de sistemas funcionan a la par con un firewall, ya que ahí se fusionaría la inteligencia del IPS con el bloqueo del firewall, aclarando que un IPS por sí solo no detiene los ataques.
- Realizar auditorías internas y con entes externos para verificar nuestra seguridad tanto perimetral como interna, verificar la seguridad en los puertos, políticas de seguridad por parte de los usuarios, como la de los administradores del sistema, obtener reportes progresivos del consumo del ancho de banda y qué servicios son los que más consumen de este recurso para compensar dicho requerimiento y así no mantengamos retardo en las respuestas por parte del servidor.
- Realizar la instalación y configuración de un firewall especializado para centrales telefónicas Elastix (propia de este producto), y mantener el direccionamiento Ip segmentado, donde no todos los funcionarios tengan acceso, principalmente dejando en otro segmento a las redes wi-fi; más aún se recomienda la formulación de una contraseña con no menos de 16 caracteres, con letras mayúsculas, minúsculas, numéricas y caracteres especiales, para así no facilitar el ataque a cualquier tipo de intruso, sea este interno o externo.
- Realizar un registro digital y actualizado de todos los eventos y sucesos ocurridos en todos los sistemas, esto incluye, servidores, usuarios, servicios y demás; así se procura, corregir errores, mantener actualizados los servicios, buscar en blog o foros actuales bugs relacionados a los sistemas o versiones para evitar futuras eventualidades y caídas de sistemas, así como la implementación de un Syslog Server y capacitaciones al personal de la institución.

REFERENCIAS

Álvarez, F. y Yépez, C. (2011). *Diseño de una red telefónica IP interna entre los colegios San José – La Salle de Guayaquil y HNO Miguel – La Salle de Quito, usando como central telefónica servidores con sistema operativo libre y software libre*. Material inédito. Universidad de Guayaquil. Ecuador.

Cáceres, J. (2014). *Análisis de vulnerabilidades en protocolos utilizados en*

centrales VoIP con IPv6 utilizando troncales SIP (trabajo de diploma inédito). Universidad de Guayaquil. Ecuador.

Christian, Z. (2013). *Implementación de servidor asterisk en la nube interna de la carrera de Ingeniería en Sistemas Computacionales*. Material inédito. Universidad de Guayaquil. Ecuador.

Landívar, E. (2008). *Comunicaciones Unificadas con Elastix*. Material inédito. Universidad de Guayaquil. Ecuador.

Rivera, P. y Poma, B. (2013). Diseño e implementación de centrales telefónicas de voz sobre IP para prácticas de análisis de tráfico, señalización, protocolos de conmutación y troubleshooting voip para uso en el laboratorio de telecomunicaciones. *Journal of Chemical Information and Modeling, 53*(9). Recuperado de: http://doi.org/10.1017/CBO9781107415425.008

Salcedo, O., López, D., y Hernández, C. (2011). Estudio comparativo de la utilización de ancho de banda con los protocolos SIP e IAX, 171–187. Material inédito. Universidad de Guayaquil. Ecuador.

Santos, G. (2008). *Asterisk-The Open Source PBX Telefonía IP mediante Asterisk PBX.* Material inédito. Universidad de Guayaquil. Ecuador.

Sotomayor, J. (2013). Análisis de vulnerabilidades de seguridad en centrales VOIP elastix a través de hacking ético. *Journal of Chemical Information and Modeling*, *53*(9), pp. 1689–1699. Recuperado de: http://doi.org/10.1017/CBO9781107415324.004