Análisis de Paquetes de Voz dentro del servidor de VoIP "Axon Virtual PBX" ¿Sistema inseguro?

Cerón, David Mauricio.
davidmauricio.ceron@gmail.com
Universidad Piloto de Colombia

***Resumen*—**En este artículo se mostrará una de las vulnerabilidades de la plataforma de VoIP "Axon Virtual PBX", asociada a la transmisión de los paquetes de voz, se realizarán pruebas montando el servidor, creando extensiones, realizando llamadas, capturando paquetes con el fin de mostrar la manera para escuchar las conversaciones. Finalmente, se indicarán soluciones con el fin de minimizar al máximo esta vulnerabilidad, y así no se afecte la actividad del negocio.

***Índice de Términos*—** *VoIP - Voz – transmisión – tramas – PBX - Confidencialidad.*

***Abstract*—** This article will show one of the "Axon Virtual PBX" VoIP vulnerabilities, acording to voice packets transmission, i will perform test to manage the server, configuring pone extensions, making calls, monitoring sniffer packets, and i will show the way to listen to conversations. Finally, solutions are indicated to minimize maximum vulnerability, with business activity affect.

***Keywords*—** *VoIP - Voice – transmission – Frames – PBX - Confidenctiality.*

I. INTRODUCCIÓN

Vivimos en una época, en la que las comunicaciones sobre internet han aumentado en forma considerable, esto debido a su menor costo de implementación, pues utilizan medios de comunicación existentes, que son usados para la transmisión de datos.

Por temas de aprovechamiento máximo de recursos, las compañias actualmente se ven obligadas a implementar soluciones que les ahorren dinero, es allí, donde nace la necesidad de la implementación de la tecnología de voz sobre protocolo de internet, ya que con este, se ahorra cantidad de infraestructura que involucra grandes costos, así como la telefonía actual pública básica conmutada.

En este artículo se hará énfasis en el servidor de VoIP llamado Axon Virtual PBX, en el que se montará un escenario de pruebas, y se realizarán captura de paquetes con el fin de escuchar las llamadas entre las extensiones, y así mismo identificar riesgos y amenazas del sistema en mención, con el fin de proteger los activos de la organización.

Finalmente, se darán soluciones que impliquen el grado de seguridad de protección del sistema, con el fin de protegerlo al máximo, o siendo el caso, pasar a implementar un sistema de voz sobre el protocolo de internet, que sea diferente, al que se ha hecho énfasis por ser gratuito.

II. VOZ SOBRE PROTOCOLO INTERNET.

VoIP, su acrónimo en inglés significa "Voice Over Internet Protocol[1]", es decir, es una tecnología que permite la emisión de voz mediante el protocolo IP, sobre redes de datos como la internet. Esta tecnología, transporta voz que ha sido procesada y encapsulada, con el fin de desarrollar una red en la

[1]Protocolo de Voz Sobre Internet.

que se envía información como voz, video o datos. Entre sus principales ventajas, radica en el aprovechamiento máximo de recursos como los servicios, así mismo como el ahorro en infraestructura innecesaria la cual está sometida la telefonía básica conmutada común.

Respecto a sus mayores inconvenientes, se destacan la seguridad y la calidad de servicio, esto debido, a que utiliza el protocolo de transporte IP (ya sea TCP o UDP), y existe la posibilidad a que dicha transmisión puede perderse antes de llegar a su destino, así mismo, como el tiempo en el que tarda el mensaje en ser emitido desde el emisor hacia el receptor, y sus pérdidas en la comunicación.

Referente a las vulnerabilidades del sistema, es la determinación de los niveles de riesgo que puede presentar una compañía de acuerdo a las amenazas, la probabilidad de que estas amenazas se materialicen y el efecto que producirá esta materialización. Para el análisis de un sistema de VoIP, se hace énfasis sobre capas en donde interactúan con la seguridad de la información, en donde se destacan captura de datos, acceso al sistema, denegación de la plataforma, entre otros.

III. DISEÑO E IMPLEMENTACIÓN DE LA TOPOLOGÍA DE RED.

Para realizar el análisis correspondiente de una trama de voz, se ha decidido montar una topología libre, en donde se instalará el servidor de VoIP Axon Virtual PBX. A continuación se describe la topología que se montó.

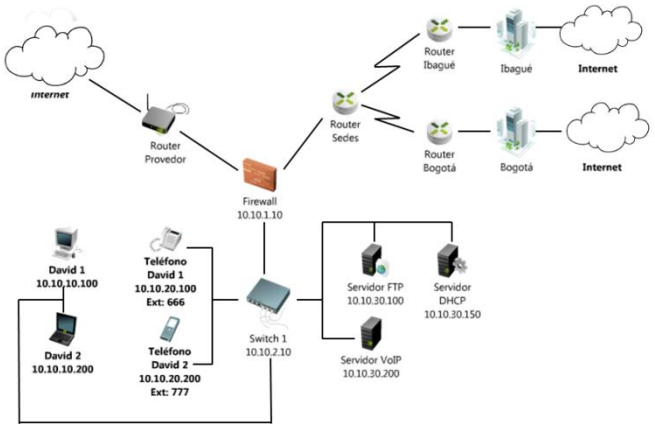

Gráfico 1. Escenario de red implementado
Fuente: Elaborado por el autor.

En la casa se tiene una conexión a internet con el proveedor de Telmex con capacidad de 1Mbps, un Router/Modem marca "Thomson" y otro marca "D-Link", se implementa un firewall (software) libre denominado Smoothwall, se tienen dos computadores de escritorio, un PC Portátil, y dos teléfonos inteligentes (iPhone y Samsung Galaxy) para simular el teléfono VoIP, ese es el escenario base con el que se realizaran pruebas.
Se ha segmentado la red con el fin de proteger y definir acorde a perfiles y roles los elementos de la red, un computador de escritorio y portátil correspondientes a usuarios normales, estos están dentro del segmento 10.10.10.0/24. Los teléfonos IP (que son simulados con teléfonos celulares de gama alta) están dentro del segmento 10.10.20.0/24, uno de estos tendrá la extensión número "666", y al otro se le configurará la extensión número "777", y finalmente, la zona de servidores en donde montará el sistema Axon Virtual PBX está dentro del segmento 10.10.30.0/24.

Referente a la configuración del Switch que recibe todo el tráfico de los tres segmentos anteriormente nombrados, no se configuró conmutación de paquetes especial, ni se hizo "Hardening[2]" de dispositivo, ni se deshabilito "Spanning Tree", este dispositivo está conectado al firewall en donde sólo se configuró una política para permitir el tráfico

[2]Método utilizado para asegurar un servidor.

entre el servidor de VoIP y los teléfonos.

Se ha decidido dibujar dentro de la topología descrita anteriormente, otros servidores que son DHCP y FTP, y además, conexión mediante enlace dedicado a dos sedes dentro del país, estas son en la ciudad de Ibagué y en la ciudad de Bogotá, esto, con el fin de simular escenarios reales de organizaciones actuales en donde se tiene implementado el sistema de VoIP mediante la plataforma Axon Virtual PBX.

IV. INSTALANDO LA PLATAFORMA, SERVIDOR DE VoIP AXON VIRTUAL PBX.

Dentro de uno de los PCs de escritorio, se decide montar el sistema Axon Virtual PBX, este computador cuenta con sistema operativo Windows 7 Ultimate, Memoria Ram de 3GB, procesador "AMD Phenom™ 8600 Triple-Core Processor 2.30 GHz", y el tipo de sistema es de 32 Bits. El aplicativo de VoIP es un ejecutable ".exe", el cual se instalará y este proceso es descrito a continuación.

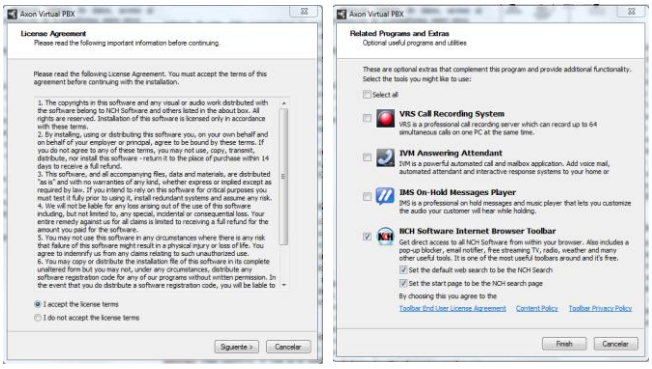

Gráfico 2. Términos de licencia y extras.
Fuente: Elaborado por el autor.

En el gráfico No.2, la imagen corresponde a aceptar los términos de licencia al instalar el aplicativo, y a la selección de los "Addons" adicionales o extras que pueden ser incluidos dentro del mismo.

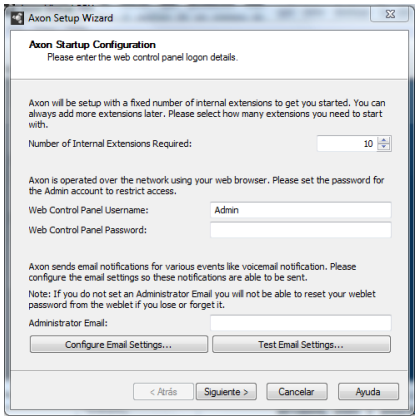

Gráfico 3. Configuración de credenciales, administración.
Fuente: Elaborado por el autor.

En el gráfico anterior se realiza la configuración correspondiente al número de extensiones requeridas por el servidor, y se definen las credenciales de usuario y contraseña para la administración Web de la plataforma.

En el siguiente Gráfico (No.4), se evidencia la interface de Logs después de haber instalado el servidor, se observa la dirección IP de la máquina, y los puertos utilizados durante la conexión, también, NATs asociados, o intercambio de información entre conexiones de las extensiones.

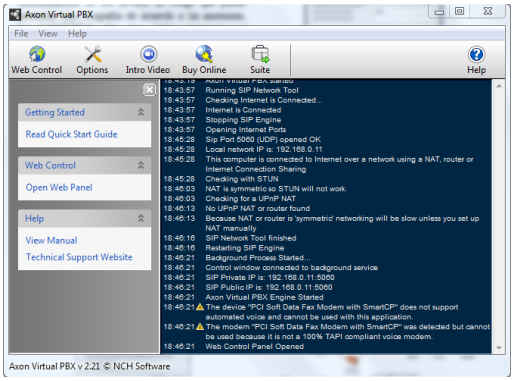

Gráfico 4. Interface de visualización de Logs.
Fuente: Elaborado por el autor.

En el gráfico No.5 de a continuación, ya es finalizada el proceso de instalación, y corresponde a la interface de gestión en donde se deben digitar las credenciales de usuario y contraseña que fueron previamente configuradas.

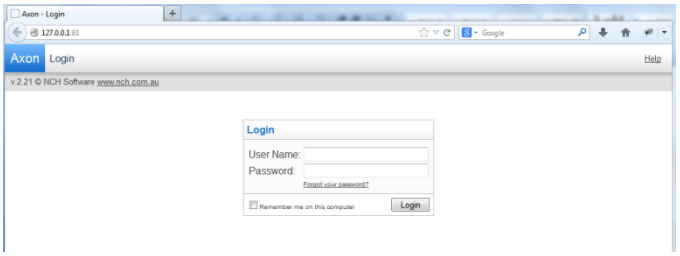

Gráfico 5. Ingreso al panel de administración.
Fuente: Elaborado por el autor.

Sobre este panel, es donde se realizará la configuración de las extensiones de los teléfonos, las números "666" y "777", también, se pueden definir características de colas de llamadas, contestadora, mensajes de voz, entre otras funcionalidades.

V. CAPTURANDO PAQUETES DURANTE LA SESIÓN DE VOZ.

Para la realización de la captura de tráfico en la interconexión, se ha instalado el aplicativo "3cx" dentro del teléfono móvil, se configuran los datos pertinentes relacionados al servidor, dirección IP del teléfono, puerto utilizado, y número de extensión. A continuación, se describe todo el proceso gráfico durante la llamada entre las extensiones.

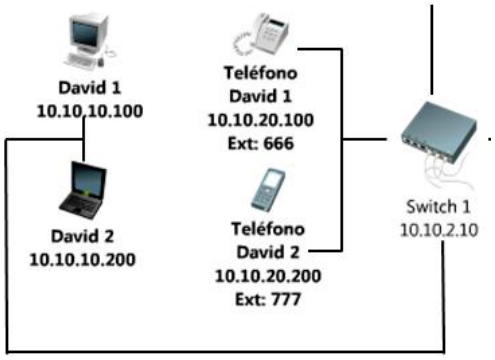

Gráfico 6. Porción de la topología, entre los dos teléfonos que se marcan entre sí.
Fuente: Elaborado por el autor.

En el anterior gráfico, se muestra una porción de la topología de red que se montó, en donde se identifican los dos teléfonos (terminales móviles), entre estos dos dispositivos se realizó la llamada, se marcó del móvil con extensión "777", al móvil con extensión "666".

Gráfico 7. Establecimiento de llamada entre ambas extensiones.
Fuente: Elaborado por el autor.

En el gráfico número 7, se evidencia que la llamada es respondida y se estableció la conexión entre ambas extensiones, durante este momento se realiza conversación entre ambos dispositivos.

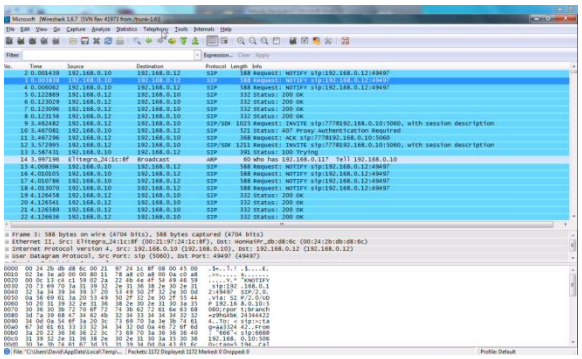

Gráfico 8. Tramas capturadas durante la sesión con el analizador de protocolos Wireshark.
Fuente: Elaborado por el autor.

En el anterior gráfico se evidencian todas las tramas de voz capturadas mientras la sesión es establecida, durante esta captura se evidencian todos los protocolos involucrados durante la conexión. Este analizador de protocolos Wireshark[3]", fue ejecutado dentro del computador en donde se instaló el servidor de VoIP Axon PBX, y allí mismo, se configuró una extensión.

[3]Analizador de protocolos con licenciamiento libre.

VI. ANÁLISIS DE LAS TRAMAS VoIP.

Durante la captura en el instante de la llamada entre ambas extensiones, se observan tramas relacionadas con los protocolos SIP, TCP, RTP, ARP y RTCP. Estas tramas pueden ser observadas en la siguiente imagen.

Gráfico 9. Distintas Tramas capturadas con sus protocolos correspondientes.
Fuente: Elaborado por el autor.

Al ver los parámetros de una trama asociada al protocolo SIP, se detallan las siguientes características:

1. Frame 4: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface 0

En este contenedor se evidencian campos relacionados con la fecha de captura (descrito en el campo "Arrival Time"), número de paquete capturado (relacionado en el campo "Frame Number"), tamaño en bytes del fragmento y de la captura (campo "Frame Length" y "Capture Length"), y protocolo involucrado de la trama ("Protocols in frame").

2. Ethernet II, Src: SamsungE_8c:b7:00 (d0:c1:b1:8c:b7:00), Dst: Elitegro_24:1c:8f (00:21:97:24:1c:8f).

En el Segundo contenedor se distinguen principalmente dos campos, ambos están relacionados con las direcciones físicas de los dispositivos que realizan la comunicación.

3. Internet Protocol Version 4, Src: 10.10.10.100 (10.10.10.100), Dst: 10.10.20.200 (10.10.20.200).

En el tercer contenedor, se distinguen campos relacionados a las cabeceras de TCP, en primer lugar se evidencia a la versión del protocolo (cuatro), longitud de la cabecera (que es de 32 bytes), las banderas (no fragmentar), el tiempo de vida del paquete (asociado al campo Time To Live), verificación de la cabecera (asociado en el campo Header Checksum), y finalmente, las direcciones IP origen y Destino desde y hacia donde se estableció la comunicación.

4. User Datagram Protocol, Src Port: 39712 (39712), Dst Port: sip (5060).

Dentro de cuarto contenedor, se evidencia el puerto fuente utilizado (39712), y el puerto destino (5060) durante la comunicación, también se destaca la longitud del campo correspondiente.

5. Session Initiation Protocol
En el quinto contenedor, se distinguen campos referentes a la cabecera del mensaje, es un resumen de todos los campos anteriormente nombrados, también se evidencia el nombre del equipo en donde está instalado el servidor y ejecutado el aplicativo.

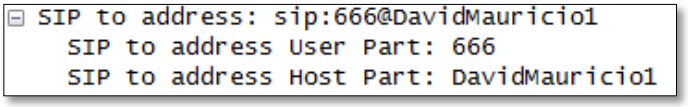

Gráfico 10. Cabecera del mensaje con sus datos.
Fuente: Elaborado por el autor.

Continuando con el análisis de las tramas de voz, se procede a revisar tramas asociadas a datos no cifrados, y haciendo uso de una característica de "VoIP Calls" referente a decodificación dentro del analizador Wireshark, se procede a seleccionar el paquetes y a decodificar el mensaje.

En el gráfico No. 11, se evidencia la trama que es seleccionada dentro del analizador de protocolos Wireshark, y en donde se describen los parámetros de tiempo de inicio, tiempo de finalización, dirección IP de quien inició la comunicación, extensión desde donde se originó y hacia donde se emitió, el número de paquetes, y finalmente el estado.

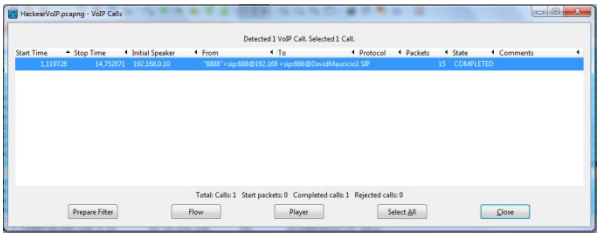

Gráfico 11. Trama correspondiente al establecimiento de llamada entre ambas extensiones.
Fuente: Elaborado por el autor.

Esta trama es seleccionada para realizar el proceso referente a decodificación.

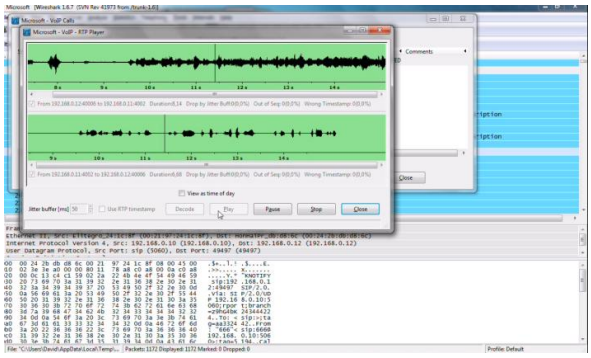

Gráfico 12. Establecimiento de llamada entre ambas extensiones.
Fuente: Elaborado por el autor.

El gráfico anterior, muestra la decodificación de la trama, con este procedimiento se logra escuchar la conversación que se realizó desde el usuario con extensión “666”, hacia el usuario con extensión “777”. Esta es una vulnerabilidad muy grande dentro de la plataforma, pues se pierde confidencialidad dentro del sistema de comunicación.

VII. CONTRAMEDIAS PARA MINIMIZAR LAS VULNERABILIDADES

Referente a lo encontrado en las tramas de voz con ayuda del analizador de protocolos, se deberá realizar “Hardening” el servidor en donde está instalado el servidor de VoIP, a este sólo debe tener acceso el administrador del sistema con sus propias credenciales, esto evitará y minimizará al máximo el riesgo referente a la instalación de aplicativos o software no deseado, pues se extrae información confidencial existente dentro de las tramas de voz, tal como se demostró durante los capítulos anteriores.

En relación a la captura realizada en donde se logró escuchar la conversación, se hace énfasis en la estructura y codificación de las tramas, el sistema investigado Axon Virtual PBX no codifica adecuadamente la comunicación entre sus usuarios, no hay seguridad en la interconexión de paquetes asociados a la voz, esta plataforma es gratuita, y no posee mayor restricción a los usuarios al hacer uso de su plataforma.

Acorde al escenario de red implementado, no hay políticas a nivel de seguridad perimetral que filtren el tráfico hacia el servidor de VoIP por puertos específicos, es recomendable configurar políticas de firewall acorde a las distintas zonas de la red con el fin de evadir posibles ataques de Ping de la muerte, u otras firmas como inyecciones SQL, ejecución de código arbitrario sobre el servidor destino, o tráfico no deseado de cualquier índole hacia el mismo con el fin de provocar uso inadecuado de los recursos de sistema.

Finalmente, resulta mucho mejor implementar sistemas de VoIP más reconocidos y que tengan el soporte necesario, que estos ambientes se destaquen por su desarrollo y su implementación en otras organizaciones, entre estos se pueden distinguir: Cisco Manager, Asterisk, y Avaya.

VIII. CONCLUSIONES

Es importante reconocer que implementar un sistema de Voz sobre IP en una organización ayuda a reducir costos drásticamente, pero al momento de realizar la implementación, no se hace énfasis en la seguridad informática que pueda afectar la actividad del negocio, se ha mostrado como un servidor gratuito como el Axon Virtual PBX, incorpora

vulnerabilidades que rompen con los pilares de la seguridad de la información, permitiendo no solo a atacantes, sino también a cualquier usuario curioso instalar un analizador de protocolos, y así capturar tráfico con el fin de escuchar conversaciones.

Es de suma importancia implementar sistemas de Voz sobre IP reconocidos, y que tengan un buen soporte, pues hay mejor cifrado de la información, los servidores por su sistema operativo evitarían la instalación de software malintencionado, los dispositivos son capaces de denegar o bloquear tráfico malicioso, y se cuenta con el apoyo directamente con el fabricante, esto manifiesta una infraestructura más fuerte al momento de implementación, y evitaría ataques que pueden ser realizados a sistemas gratuitos como el Axon Virtual PBX .

Para asegurar y reducir al máximo los riesgos identificados, no sólo se debe hacer énfasis en el servidor de VoIP, hay que tener en cuenta que en seguridad hay que pensar en varias cosas durante el mismo momento, es decir, se recomienda implementar dispositivos de red utilizados para funciones específicas, se aconseja implementar firewall para filtrado de tráfico, dispositivos IDS para detectar intrusos, dispositivos IPS para prevenirlos, e implementación de canales alternos al principal de comunicación, por si es causada una denegación de servicio, todos estos elementos son alternos al sistema de VoIP, pero trabajan en conjunto, todo para lograr el objetivo de no afectar la actividad del negocio.

IX. REFERENCIAS

[1] NHC SOFTWARE, “Technical Support Axon”, disponible en la página web: http://www.nch.com.au/pbx/support.html

[2] INTECO-CERT, Instituto nacional de tecnologías de la comunicación, documento de vulnerabilidad denominado “Vulnerabilidad en NCH Software Axon Virtual PBX (CVE-2009-4038)”.

[3] GARAIZAR, Sagarminaga Pablo, “Ataques de denegación de servicio en VoIP”, El blog de txipi.

[4] GUTIÉRREZ, Gil Roberto, “Seguridad en VoIP: Ataques, amenazas y riesgos.”, Documento de investigación Universidad de Valencia España, página 33 a 35.

[5] CRUZ Forero Giovanni, RINCÓN Alex Ricardo, RODRÍGUEZ Rodríguez Daniel, ESCOBAR Daniel, “Busy Tone Group”, Seguridad y vulnerabilidades en servidores de VoIP, disponible en: http://busy-tone.org/

[6] GÓMEZ, Celis Mónica Lorena, “Definición de políticas de seguridad para la red VoIP que presta el servicio de voz local en Gilat Colombia S.A”, Ficha tipográfica disponible en: http://goo.gl/naqeNG

[7] GÓMEZ Martín Pedro Pablo, documentación en línea, “Voz sobre IP VoIP”, ítem funcionamiento de VoIP.

[8] ESCALANTE Maribel, Trabajo de grado “Estudio de factibilidad técnica para la migración parcial o total de la red telefónica TDM internacional de Cantv a voz sobre IP”, http://www.oocities.org/es/mari0411ve/TEG1.htm

[9] ERB, Markus. Publicación en linea WordPress “Gestión de riesgo en la seguridad informática”, citado el 18 de Octubre de 2012, disponible en http://goo.gl/wVkHYx

Autor.

David Mauricio Cerón Aros
Ing. de Telecomunicaciones.
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia