Polo del Conocimiento

Pol. Con. (Edición núm. 7) Vol. 2, No 6
Jun. 2017, pp. 42-64
ISSN: 2550 - 682X
DOI: 10.23857/pc.v2i6.127

Recepción: 20 / 04 / 2017
Aceptación: 20 / 05 / 2017
Publicación: 15 / 06 / 2017

Ciencias Informáticas

Artículo de Investigación

Encontrar y solucionar las vulnerabilidades en las comunicaciones de voz sobre IP de un sistema telefónico de un call center

Find and resolve vulnerabilities in voice over IP communications from a telephone system in a call center

Encontrar e corrigir vulnerabilidades em comunicações de voz através do sistema de call center telefone IP

Eduardo S. Cruz-Ramírez [I]
escruz@espol.edu.ec

Ivette K. Carrera-Manosalvas [II]
ivette.carrera@ug.edu.ec

Ginger V. Saltos-Bernal [III]
gvsaltos@espol.edu.ec

Correspondencia: ivette.carrera@ug.edu.ec

· Ingeniero en Ciencias Computacionales, Magister en Seguridad Informática Aplicada, Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador.

II. Ingeniera en Telemática, Master of Cyber Forensics and Security, Magister en Seguridad Informática Aplicada, Universidad de Guayaquil, Guayaquil, Ecuador.

III. Ingeniera en Telemática, Master of Science in Forensic Information Technology, Magister en Seguridad Informática Aplicada, Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador.

Resumen

El presente trabajo muestra el desarrollo de un análisis de vulnerabilidades a la seguridad informática de los equipos tecnológicos dedicados a las comunicaciones telefónicas de un call center.

El análisis de vulnerabilidades se lo realiza mediante el uso de herramientas especializadas en analizar debilidades en la seguridad informática de las comunicaciones telefónicas. Estas aplicaciones permiten realizar diferentes tipos de ataques informáticos, tales como: ataques de reconocimiento, intercepción, fuerza bruta y denegación de servicios. Las vulnerabilidades detectadas son explotadas, demostrando el perjuicio o daño al que se enfrenta la compañía teniendo su infraestructura de comunicaciones telefónica sin las medidas necesarias de seguridad informática.

Posteriormente, se implementan soluciones de seguridad informática en la infraestructura de comunicaciones, tales como: encriptación en las comunicaciones de VoIP, túneles VPN, listas de acceso en las extensiones telefónicas, seguridad perimetral, detección de intrusos; estas medidas mitigan las amenazas detectadas durante el proceso de detección de debilidades informáticas, reduciendo el riesgo tecnológico al que se encuentra expuesto la empresa.

Finalmente, se realizan pruebas de seguridad informática sobre las implementaciones adoptadas en la infraestructura de comunicación de VoIP, con la finalidad de verificar la efectividad de las medidas incorporadas.

Palabras clave: Escaneo de vulnerabilidades; voz sobre IP; call center; ataques informáticos; amenazas.

Abstract

This paper shows a vulnerabilities scan to the information security of technologic equipment involved in the telephony communications of a call center.

Vulnerabilities scan is done by using specialized tools in weakness analysis to information security of telephony communications. These applications allow to do different types of information attacks, such as: recognition, interception, brute force and denial of services. The vulnerabilities detected are exploited, demonstrating injury or damage to the company faced having its communications infrastructure without required steps on information security.

Later, I implement information security solutions in the communications infrastructure such as: communications VoIP encrypted, VPN tunnels, access control list in extensions, perimeter security, intrusion detection; these steps mitigate threats detected during the weakness detection, it will reduce technology risk in the company.

Finally, I do security information tests over the steps implemented in the VoIP communication infrastructure. It's to verify the steps implemented.

Key words: Vulnerabilities scan; voice over IP; call center; information attacks; threats.

Resumo

Este artigo apresenta o desenvolvimento de uma análise de vulnerabilidades de segurança do computador de equipamentos tecnológicos dedicados a comunicações telefónicas de um call center.

análise de vulnerabilidades é realizada utilizando ferramentas especializadas para analisar os pontos fracos em segurança de computadores de comunicações telefónicas. Estas aplicações permitem diferentes tipos de ataques informáticos, tais como ataques de reconhecimento, interceptação, força bruta e negação de serviço. vulnerabilidades detectadas são exploradas, demonstrando lesão ou dano para a empresa enfrenta com sua infra-estrutura de comunicações telefónicas sem as medidas de segurança necessárias.

Posteriormente, soluções de TI de segurança na infra-estrutura de comunicações, como implementado: a criptografia de VoIP de comunicação, túneis VPN, listas de acesso de ramais telefônicos, perímetro de segurança, detecção de intrusão; Estas medidas mitigar as ameaças detectadas durante as fraquezas de computador processo de detecção, reduzindo o risco tecnológico a que a empresa está exposta.

Finalmente, o teste de implementações adotadas na infraestrutura de comunicação VoIP, a fim de verificar a eficácia das medidas de segurança construídos são feitas.

Palavras chave: Varredura de vulnerabilidades; voz sobre IP; call center; ataques a computadores; ameaças.

Introducción.

Los call centers han desarrollado su plataforma de productos y servicios sobre una infraestructura de comunicaciones de VoIP, por lo tanto, durante su permanencia en el mercado ha brindado los siguientes beneficios a sus afiliados:

- Ventas, mediante la técnica del Telemercadeo.
- Servicio de asistencia médica, utilizada por los afiliados para comunicar sus emergencias mediante llamadas telefónicas.
- Encuestas de satisfacción, mediante llamadas telefónicas a los afiliados consultándoles sobre la calidad del servicio recibido.

La organización utiliza centrales telefónicas con tecnología basada en software libre en su infraestructura de comunicaciones, por consiguiente, ha realizado interconexiones con la red telefónica de proveedores de telefonía fija y móvil.

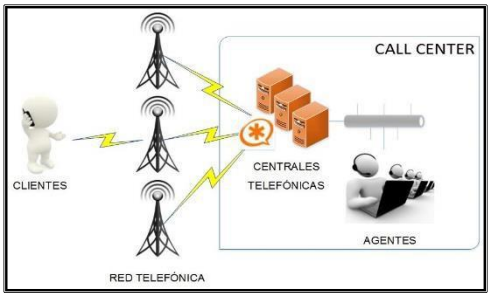

Figura 1 Diagrama de interconexión del call center con la red telefónica

Además, la telefonía de **VoIP** ha sido utilizada para establecer comunicación entre las extensiones telefónicas internas de las distintas filiales de la compañía, esto ha sido posible al utilizar como medio de comunicación el Internet.

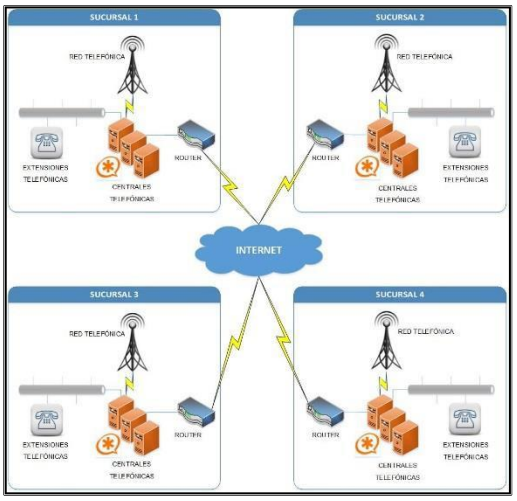

Figura 2 Diagrama de interconexión telefónica entre las distintas filiales

Las centrales telefónicas de la organización tienen la funcionalidad de generar reportes denominados CDR, los cuales contienen información relacionada con los eventos de una llamada tales como: fecha, hora de inicio, duración, número de origen, número de destino. Estos reportes son contrastados con la facturación que recibe mes a mes el departamento administrativo para verificar los consumos telefónicos, por consiguiente, esta validación ha dado alerta a las autoridades sobre los excesivos consumos telefónicos en llamadas locales, nacionales, celulares e internacionales.

El análisis de los consumos excesivos muestra que las llamadas telefónicas han sido realizadas por extensiones de las centrales telefónicas, pero no necesariamente por los operadores del call center, por lo tanto, los números destinos registrados en el CDR no corresponden a las bases de datos de números telefónicos gestionadas por los operadores ni existen grabaciones de audio de estas llamadas telefónicas. Esto hace presumir que la seguridad de las cuentas que se autentican a las centrales telefónicas ha sido vulnerada o presentan una debilidad de configuración, por consiguiente, las amenazas internas o externas se han aprovechado de las debilidades informáticas con la finalidad de obtener llamadas gratuitas que no corresponden a los fines del negocio de la organización.

La organización cuenta con suficientes líneas telefónicas para realizar sus actividades, sin embargo, han existido ocasiones en las cuales se ha evidenciado la indisponibilidad de canales telefónicos al momento de realizar llamadas por parte de los operadores, esto es, debido a los posibles ataques informáticos de denegación de servicio que pueden sufrir las centrales telefónicas.

Las problemáticas descritas han generado pérdidas económicas considerables para la organización, evidenciada en la facturación telefónica generada por los proveedores de telefonía fija y celular, no obstante, la compañía pretende reducir los riesgos informáticos a los cuales se enfrenta su infraestructura de comunicación telefónica.

Materiales y métodos.

La metodología de hacking ético que se utilizará es el de caja blanca, en el cual se simularán ataques de seguridad informática con herramientas especializadas, pero previamente conociendo gran parte de información técnica que tiene la organización.

El proceso que se llevará a cabo en el análisis de vulnerabilidades se la ha proyectado teniendo en consideración las siguientes fases:

- Recopilación de Información
- Búsqueda de Vulnerabilidades
- Explotación de Vulnerabilidades

Luego de la aplicación de esta metodología, se realizará un proceso de remediación de las vulnerabilidades detectadas empleando las siguientes fases:

- Análisis de Remediación
- Implementación de soluciones

- Análisis de resultados

3. Análisis de Infraestructura

La infraestructura de comunicaciones del call center está compuesta por los siguientes elementos:

- Teléfonos basados en hardware
- Teléfonos basados en software
- Los conmutadores
- Los servidores

Estos elementos tecnológicos se encuentran operando en 2 segmentos de red claramente identificados. En la localidad de Guayaquil se encuentra configurado el segmento de red 192.168.4.0/24 y en la localidad de Quito se encuentra configurado el segmento de red 192.168.1.0/24. En cada localidad existen 2 centrales telefónicas, las direcciones IP de las centrales de Guayaquil son 192.168.4.230 y 192.168.4.188, mientras que las direcciones IP de las centrales de Quito son la 192.168.1.6 y 192.168.1.7, además, existe un enlace de datos entre las localidades que facilita la comunicación entre Guayaquil y Quito.

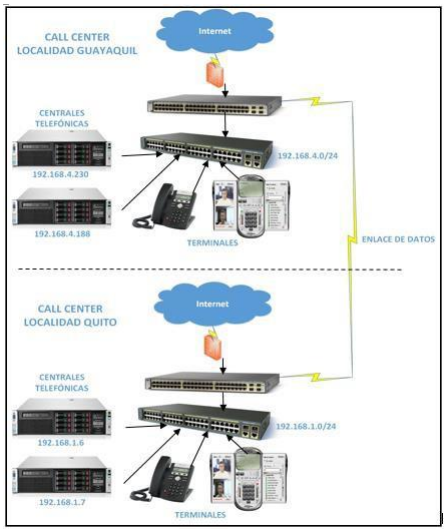

Figura 3 Arquitectura de comunicaciones del call center

4. Diseño e Identificación de Vulnerabilidades

En primer lugar, se realizará un diseño de los vectores de ataques que se desplegarán hacia las centrales telefónicas, este diseño permitirá tener una estructura de los ataques que se emplearán en la infraestructura de comunicaciones del call center.

Figura 4 Diseño de pruebas de identificación de vulnerabilidades

4.1. Escenario

El computador será la herramienta principal para desempeñar el rol de un atacante, esto es, porque tiene instalado todas las herramientas que se utilizarán durante el análisis de vulnerabilidades. La distribución Linux que se utilizará es “KALI LINUX” en su versión “1.1.0”, este sistema cuenta con las aplicaciones más populares para realizar un hacking ético hacia diferentes servicios informáticos.

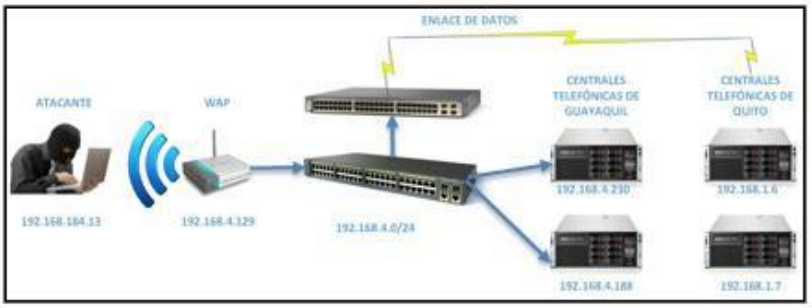

Figura 5 Escenario para el despliegue de los vectores de ataques

4.2. Ataques de Reconocimiento

Esta fase es una etapa de preparación, en la que se pretende obtener toda la información necesaria de la infraestructura de comunicaciones previa al despliegue de los ataques informáticos.

Reconocimiento de versiones

Se procederá a utilizar la herramienta "svmap" para identificar el software de las centrales telefónicas, esta aplicación envía un requerimiento de inicio de sesión SIP "INVITE" al objetivo, por consiguiente, en el intercambio de mensajes para establecer el inicio de sesión se revelará información del aplicativo de VoIP que está utilizando. Como podemos observar en la imagen siguiente, el software que tienen instaladas las centrales telefónicas es "Asterisk" en su versión "1.6.2.20" y "1.6.0.6".

```
root@kali:~# svmap 192.168.1.7 -m INVITE
| SIP Device       | User Agent            | Fingerprint |
-------------------------------------------------------------
| 192.168.1.7:5060 | Asterisk PBX 1.6.2.20 | disabled    |
```

Figura 6 Reconocimiento de versiones del software de la central telefónica "192.168.1.7"

Reconocimiento de puertos y servicios

El escaneo de puertos y servicios se llevará a cabo con la aplicación “nmap”, utilizando la implementación gráfica de esta herramienta denominada “zenmap”.

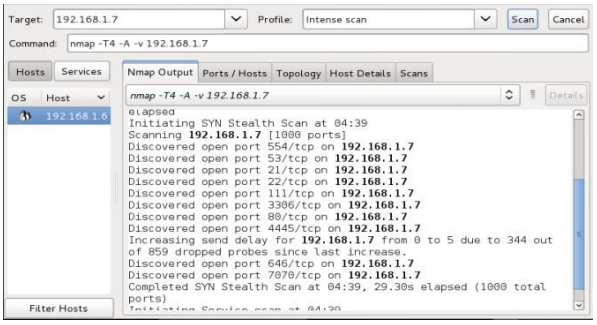

Figura 7 Escaneo de puertos a la central telefónica “192.168.1.7”

El reconocimiento realizado con la herramienta “zenmap” revela que los siguientes puertos bien conocidos se encuentran habilitados en las centrales telefónicas:

Puerto (TCP)	Descripción
21	FTP
22	SSH, SFTP, SCP
53	DNS
80	HTTP
111	SunRPC
113	Ident
139	NetBIOS
554	RTSP
3306	MYSQL

Tabla 1 Puertos bien conocidos encontrados durante el escaneo de puertos

Reconocimiento de extensiones

Para realizar este reconocimiento se procederá a utilizar la herramienta “svwar”. Esta herramienta realiza un escaneo a la central telefónica objetivo, enviando peticiones SIP de inicio de sesión “INVITE” a un rango de extensiones, el rango especificado en los parámetros de la

ejecución del comando es un listado de extensiones de las cuales se presume que se encuentran configuradas en la central telefónica. Como podemos apreciar en la imagen siguiente, se ha iniciado utilizando la aplicación "svwar" con un rango de extensiones de 3 dígitos.

Efectivamente, ante esta ejecución se detecta que las centrales telefónicas tienen configuradas extensiones con 3 dígitos, además, muestra cuales son las extensiones configuradas del rango inicialmente proporcionado.

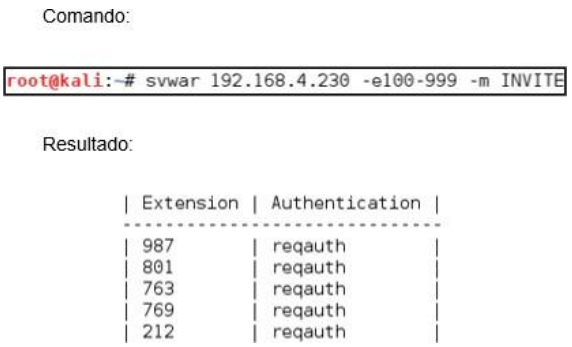

Figura 8 Reconocimiento de extensiones en la central telefónica "192.168.4.230"

4.3. Ataques de intercepción

En esta fase se realizará un ataque de intercepción, capturando la información que se transmite mediante el protocolo SIP en las comunicaciones de VoIP sobre la red de datos de la organización. Para lograr este objetivo inicialmente se utilizará la herramienta "ettercap", la cual permite realizar un envenenamiento ARP, por consiguiente, podremos husmear los paquetes de datos que atraviesan la red de datos desde nuestro computador atacante.

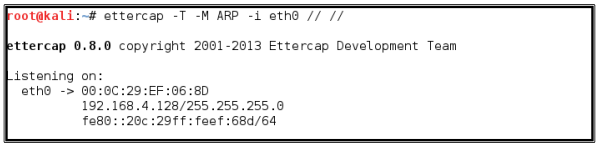

Figura 9 Envenenamiento ARP con la herramienta "ettercap"

Luego de realizar el envenenamiento ARP, se procederá a capturar todos los paquetes que están atravesando la red de datos, para ello se utilizará la herramienta “wireshark”, la cual nos permite visualizar toda la información de los paquetes capturados, datos como: la dirección IP origen, la dirección IP destino, el protocolo del paquete, etc. Finalmente, la herramienta cuenta con una funcionalidad para extraer los paquetes que son utilizados por las comunicaciones de VoIP, por consiguiente, se puede decodificar la información que llevan los paquetes utilizados en las comunicaciones telefónicas y reproducir el audio de las conversaciones que mantiene el personal de la organización.

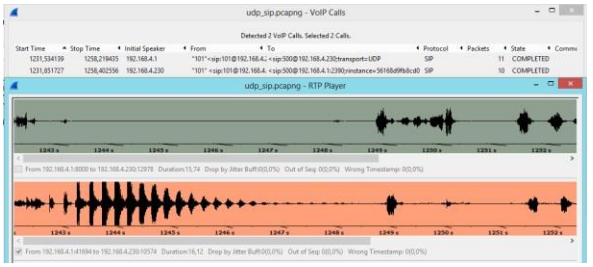

Figura 10 Captura de paquetes en las comunicaciones de VoIP y reproducción de audio de las conversaciones del personal de la organización.

4.4. Ataques de Denegación de Servicios

La herramienta que se utilizará para realizar este ataque informático es “inviteflood”. Esta aplicación tiene la capacidad de enviar constantemente una gran cantidad de peticiones de inicio de sesión “INVITE” de una extensión SIP hacia una central telefónica, causando una sobrecarga en el procesamiento de estos requerimientos y originando la indisponibilidad del servicio de comunicaciones telefónicas.

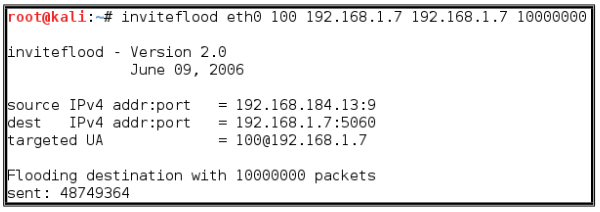

Figura 11 Ataque de denegación de servicio a la central telefónica "192.168.1.7"

La CLI de cada central telefónica "Asterisk" muestra los requerimientos continuos de sesión enviados por la herramienta "inviteflood", además, se pudo apreciar en el monitoreo la extensión utilizada para desplegar estos ataques.

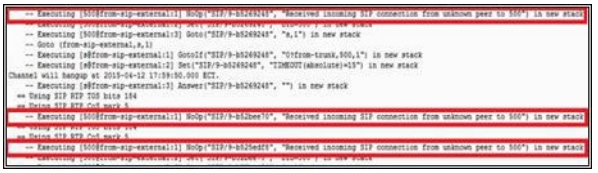

Figura 12 CLI de la central telefónica "192.168.1.7" mostrando el ataque de denegación de servicios

La carga promedio de cada servidor de la central telefónica se presenta considerablemente elevada, esta medida nos indica la ocupación de los recursos de hardware tales como: procesador del sistema, disco duro y otros recursos. La sobrecarga en el servidor de la central telefónica es ocasionada por el proceso "Asterisk", quien se encuentra tratando de atender todos los requerimientos de inicio sesión SIP, pero los recursos de hardware no son suficientes para atender esta gran cantidad de peticiones, generando una saturación en el servidor. Durante la ejecución del ataque, el personal de sistemas no pudo operar el servidor de una manera adecuada.

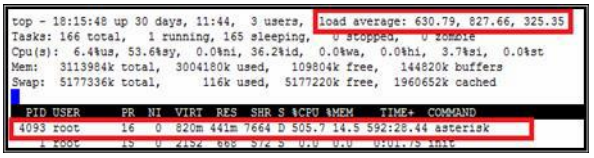

Figura 13 Carga promedio de la central telefónica "192.168.1.7", durante el ataque de denegación de servicios

Finalmente, durante la ejecución del ataque de denegación de servicios, el personal administrativo y los operadores del call center no pudieron utilizar los servicios de comunicaciones para realizar sus respectivas llamadas telefónicas.

Figura 14 Estado de los teléfonos durante el ataque de denegación de servicios

4.5. Ataques de Fuerza Bruta

Inicialmente se procederá a crear un diccionario con combinaciones de claves numéricas, las cifras que se generarán van de 3 a 10 dígitos, por consiguiente, el número total de combinaciones que se crearán es de once mil ciento once millones ciento once mil, además, esto representa para el almacenamiento un diccionario de claves cuyo tamaño es de 112 GB.

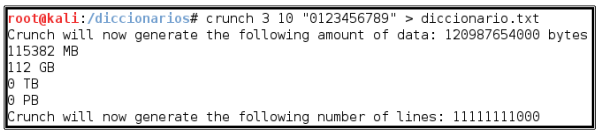

Figura 15 Generación del diccionario de claves numéricas

Una vez generado el diccionario, lo siguiente que se procederá a realizar es el ataque de fuerza bruta usando el diccionario de claves numéricas; para realizar este ataque se utilizará la herramienta "svcrack", la cual opera realizando el proceso de autenticación SIP de una extensión con un diccionario de claves, por consiguiente, para la ejecución del comando se especificará una extensión SIP válida que previamente hemos descubierto en los ataques de reconocimiento.

```
root@kali:~# svcrack -u 101 -d /diccionarios/diccionario.txt 192.168.4.230
| Extension | Password |
-----------------------
| 101       | 101      |
```

Figura 16 Ataque de fuerza bruta basada en diccionario a la extensión "101" de la central "192.168.4.230"

4.6. Explotación de Vulnerabilidades

Con los datos de usuario y clave de las extensiones SIP encontradas en el análisis de vulnerabilidades podemos autenticarnos a la central telefónica utilizando esta información, como podemos ver en la imagen siguiente nos autenticaremos con un teléfono basada en software a la central telefónica "192.168.4.230" desde la máquina atacante y poder realizar llamadas.

Figura 17 Autenticación exitosa en la central "192.168.4.230" y generación de llamadas telefónicas desde la máquina atacante.

5. Implementación de Soluciones de Seguridad Informática

5.1. Actualización del Sistema

Se realizará la actualización de las versiones de todos los componentes de software instalados en los servidores de las centrales telefónicas, esto se logrará mediante la instalación de la distribución Linux "FreePBX DISTRO" en su última versión estable "6.12.65", sustituyendo la anterior versión del sistema de telefonía. Esta distribución contiene las más recientes actualizaciones de "Asterisk" en su versión "13.3.2" y "FreePBX" en su versión "12.0.63"", además, la distribución está orientada a brindar servicios de telefonía segura a las organizaciones, por lo tanto, sus módulos están destinados a brindar medidas necesarias de seguridad informática para manejar comunicaciones telefónicas seguras.

5.2. Cifrado en las comunicaciones de VoIP

Inicialmente se procederá a crear la autoridad de certificación en la central telefónica, esta entidad será la encargada de la emisión y revocación de los certificados digitales. La aplicación "FreePBX" ya cuenta con un módulo para la creación de la autoridad certificadora y se lo utilizará especificando la dirección IP del servidor, el nombre de la organización y una clave secreta.

Figura 18 Emisión de certificado para la extensión "500" de la central telefónica "192.168.4.230"

Las extensiones telefónicas por defecto tienen la capacidad de manejar protocolos de transporte UDP y TCP, sin embargo, se procederá a habilitar el soporte para que las

comunicaciones de VoIP puedan manejar el protocolo de transporte seguro TLS en la transmisión de la información. En las configuraciones avanzadas del protocolo SIP se habilitará el parámetro "SIP encryption" en "yes" y se utilizará el parámetro "tlsenable" en "yes" para establecer el soporte para el cifrado en la transmisión de la información, además, en los parámetros de la extensión se configurará la opción "Transport" en "All - TLS Primary" para especificar que el transporte solo será mediante este protocolo, también se habilitará el cifrado del protocolo RTP mediante el protocolo SRTP para asegurar la comunicación en tiempo real que se dará en una conversación telefónica.

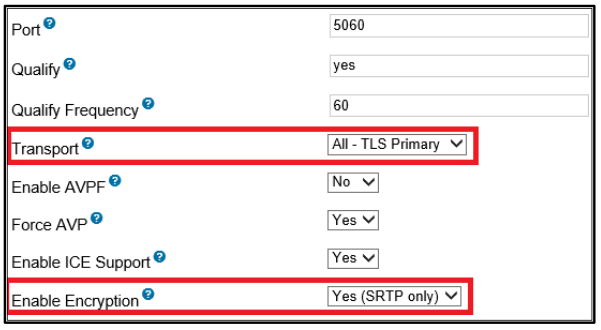

Figura 19 Configuración del protocolo TLS y SRTP en la extensión telefónica "500" de la central telefónica "192.168.4.230"

5.3. Listas de Control de Accesos

La medida de seguridad se basa en denegar inicialmente el acceso a todas las direcciones IP, posteriormente, se agregarán las direcciones IP que van a estar autorizadas a utilizar esta extensión, por consiguiente, no cualquier dispositivo podrá usar cualquier extensión. Por ejemplo, un operador de call center utiliza la extensión 500 creada en la central telefónica cuya dirección IP es "192.168.4.230" y el computador donde labora el operador tiene dirección IP "192.168.4.5", por la tanto, la lista de acceso que se configurará en el archivo de configuración de las extensiones SIP en la central telefónica denominado "sip.conf" o utilizando la interfaz gráfica de configuración del "FreePBX".

Figura 20 Configuración de la ACL en la extensión "500" de la central telefónica "192.168.4.230"

5.4. Políticas de contraseñas

La aplicación de "FreePBX" al momento de crear una extensión SIP contribuye a crear una contraseña aleatoria más robusta por defecto de 32 caracteres, es decir, tiene una dimensión de 256 bits y es una combinación de letras y números; sin embargo, los administradores de la central telefónica pueden cambiar esta contraseña por la política que tengan definida en sus procedimientos.

Figura 21 Contraseña generada por la aplicación "FreePBX" en la creación de una extensión

5.5. Seguridad perimetral

La implementación que se realizará es de una VPN IPsec para la comunicación de datos entre las centrales de Guayaquil y México, para lograr este objetivo se utilizará la distribución IPCop, la cual está basada en Linux y permite realizar túneles VPN con el protocolo IPsec, entre los parámetros de configuración, se establecerá los protocolos de criptografía que se utilizarán para asegurar el flujo de los paquetes, garantizar la autenticación mutua y establecer los parámetros de cifrado, además, se establecerá una clave previamente compartida para establecer la comunicación entre las dos filiales.

Figura 22 Configuración de los parámetros criptográficos de la VPN IPsec

5.5. Implementación del IPS

El IPS que se utilizará es la solución denominada “Fail2ban”, esta aplicación previene ataques de fuerza bruta y denegación de servicio basado en la parametrización de la cantidad de intentos de ataques “maxretry” y bloqueará el acceso a la dirección IP atacante por el lapso estipulado en el parámetro “bantime”. Como se muestra en la imagen siguiente, la política establece que hay un máximo de 5 intentos y en caso de ser detectado estará bloqueado por 30 minutos, también tiene la capacidad de manejar alertas vía correo electrónico a los administradores del sistema en caso de que se aplique un bloqueo.

```
[asterisk-iptables]
enabled  = true
filter = asterisk-security
action   = iptables-allports[name=SIP, protocol=all]
           sendmail[name=SIP, dest=none@yourpbx.com, sender=none@yourpbx.com]
logpath  = /var/log/asterisk/fail2ban
maxretry = 5
bantime = 1800
```

Figura 23 Políticas de configuración de la aplicación “Fail2ban”

La detección de los ataques se basa en la lectura de los logs de la aplicación que se busca proteger, por consiguiente, el “Fail2ban” analizará los logs de “Asterisk” en función de unos filtros predefinidos, por consiguiente, detectará si la aplicación está siendo víctima de un ataque de fuerza bruta o de denegación de servicios.

Resultados.

La fase de pruebas de seguridad ha demostrado la efectividad de las medidas de seguridad informática aplicadas sobre las comunicaciones de VoIP, por lo tanto, para cada tipo de ataque existe una medida de seguridad que dificulta el acceso a la información por parte de las amenazas.

Para los ataques de intercepción, la medida de seguridad informática es:

Cifrado en las comunicaciones de VoIP.

Para los ataques de fuerza bruta basadas en diccionarios, las medidas de seguridad informática son:

Políticas de contraseña.

Listas de control de Acceso ACLs.

Implementación del IPS (Fail2ban).

Para los ataques de denegación de servicios, la medida de seguridad informática es:

Implementación del IPS (Fail2ban).

Estas medidas de seguridad previenen que el atacante pueda obtener información sensible en las comunicaciones de VoIP y de esta manera poder sacar provecho de las vulnerabilidades para beneficio propio.

Conclusiones.

El análisis de vulnerabilidades aplicado a la infraestructura de comunicaciones de VoIP demostró que existen vulnerabilidades informáticas en las centrales telefónicas, por lo tanto, la organización se encuentra expuesta a un riesgo informático de alto impacto sobre las

operaciones de la compañía. Las vulnerabilidades informáticas encontradas demuestran que las amenazas pueden aprovechar estas debilidades para obtener provecho de las mismas, inclusive obteniendo beneficios económicos y causando un perjuicio a la organización.

Las vulnerabilidades detectadas en la infraestructura de comunicaciones de VoIP atentan contra las metas de la seguridad informática en la organización que son la disponibilidad, la integridad, la confidencialidad y la autenticidad.

Las medidas de seguridad aplicadas a la infraestructura de comunicaciones VoIP tales como: Cifrado en las comunicaciones, Uso de ACL's, Políticas de contraseña, Seguridad perimetral utilizando túneles IP sobre VPN, Implementación de IPS han sido verificadas respecto a su efectividad mediante pruebas de seguridad informática aplicada, las mismas que demuestran que las medidas de seguridad solucionan los problemas detectados en el análisis de vulnerabilidades previamente realizado.

Recomendaciones

Mantener revisiones periódicas de las nuevas actualizaciones de seguridad sobre los componentes que pueden ser aplicados a la infraestructura de comunicaciones telefónicas.

Establecer una planificación de auditorías sobre la seguridad informática de la infraestructura de comunicaciones VoIP.

Realizar una campaña de concientización al personal de la organización sobre la importancia de la seguridad de la información, esto es, con la finalidad de que el personal de la organización sea parte de las normas y procedimientos para la gestión de la seguridad informática.

Realizar una evaluación del riesgo informático al que se encuentra la infraestructura de comunicaciones de VoIP, esto es, con la finalidad de elaborar un plan de medidas para mitigar los riesgos detectados.

Implementar un sistema de gestión de la seguridad de la información basada en estándares internacionales como por ejemplo la norma: ISO 27001-2013.

Bibliografía.

[1] Gutiérrez Gil, R. «Universidad de Valencia,» [En línea]. Available: http://www.uv.es/~montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf, fecha de consulta marzo del 2015.

[2] Misfud Talón, E. , Lerma-Blasco, R. V. , Servicios en Red, Aravaca (Madrid): McGraw-Hill/Intermaericana de España, S.A.U, 2013.

[3] Villalón, J. L. , «Security Art Work,» 3 Marzo 2008. [En línea]. Available: http://www.securityartwork.es/2008/03/03/voip-protocolo-sip/, fecha de consulta marzo del 2015.

[4] «Elastix Tech,» 2015. [En línea]. Available: http://elastixtech.com/protocolo-iax/, fecha de consulta marzo del 2015.

[5] 3CX, «3CX,» 2015. [En línea]. Available: http://www.3cx.es/voip-sip/telefono-voip/, fecha de consulta marzo del 2015.

[6] NightRang3r, «backtrack-linux,» [En línea]. Available: http://www.backtrack-linux.org/wiki/index.php/Pentesting_VOIP, fecha de consulta marzo del 2015.

[7] González, P. , Sánchez, G. , Soriano, J. M. , Pentesting con Kali, 0xword, 2013.

[8] Astudillo, K. , HACKING ÉTICO 101, Guayaquil: Amazon, 2013.

[9] Almeida, J. , «Blog personal de Jaime Almeida,» 11 07 2012. [En línea]. Available: http://juanelojga.blogspot.com/2012/07/sip-tls-y-srtp-en-elastix.html, fecha de consulta marzo del 2015.

[10] Davenport, M. , «Asterisk,» 3 12 2014. [En línea]. Available: https://wiki.asterisk.org/wiki/display/AST/Secure+Calling+Tutorial, fecha de consulta marzo del 2015.