

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

**“ENCONTRAR Y SOLUCIONAR LAS VULNERABILIDADES EN
LAS COMUNICACIONES DE VOZ SOBRE IP DEL CALL CENTER
MEDIASIST”**

TESIS DE GRADO

Previo a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

EDUARDO SEGUNDO CRUZ RAMÍREZ

GUAYAQUIL - ECUADOR

AÑO

2015

AGRADECIMIENTO

A Dios, por brindarme la vida; a mis padres, que son un gran ejemplo de superación, por su constante e incondicional ayuda; a mis familiares y amigos, por compartir sus importantes consejos para la obtención de mis logros académicos.

Eduardo Cruz Ramírez.

DEDICATORIA

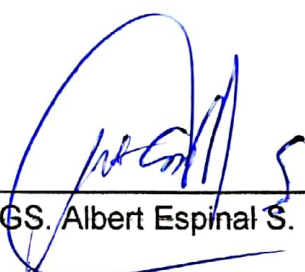
A todas las personas que participaron en mi desarrollo profesional, quienes esperan mi constante contribución al desarrollo tecnológico del país con los conocimientos adquiridos en mi formación académica.

Eduardo Cruz Ramírez.

TRIBUNAL DE GRADUACIÓN

MGS. Lenin Freire C.

DIRECTOR MSIA



MGS. Albert Espinal S.

DIRECTOR



MGS. Robert Andrade T.

MIEMBRO PRINCIPAL DEL TRIBUNAL

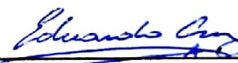
MGS. Néstor Arreaga A.

MIEMBRO SUPLENTE DEL TRIBUNAL

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la **Escuela Superior Politécnica del Litoral**”

(Reglamento de Graduación de la ESPOL).



Eduardo Cruz Ramírez

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 en la empresa MEDIASIST S.A, la compañía está dedicada a brindar servicios de asistencia médica a sus afiliados mediante un call center.

Además se realiza una descripción de los elementos activos que intervienen en las comunicaciones de **VoIP** en la organización. Luego de realizar esta identificación, se estructura los vectores de ataques dirigidos a vulnerar la seguridad informática de la infraestructura de comunicaciones, los vectores de ataques se constituyen en una planificación para realizar el análisis de vulnerabilidades. El análisis de vulnerabilidades se lo realiza mediante el uso de herramientas especializadas en analizar debilidades de la seguridad informática de las comunicaciones telefónicas. Estas aplicaciones permiten realizar diferentes tipos de ataques informáticos, tales como: ataques de reconocimiento, interceptación, 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.

ÍNDICE GENERAL

AGRADECIMIENTO	ii
DEDICATORIA	iii
TRIBUNAL DE GRADUACIÓN	iv
DECLARACIÓN EXPRESA	v
RESUMEN.....	vi
ÍNDICE GENERAL.....	viii
ABREVIATURAS Y SIMBOLOGÍA	xii
GLOSARIO	xiv
ÍNDICE DE FIGURAS.....	xvii
ÍNDICE DE TABLAS	xxiii
INTRODUCCIÓN	xxiv
CAPÍTULO 1.....	1
GENERALIDADES	1
1.1 Antecedentes.....	1
1.2 Descripción del problema	4
1.3 Solución propuesta.....	5
1.4 Objetivos generales.....	7

1.5	Objetivos específicos.....	8
1.6	Metodología.....	9
CAPÍTULO 2.....		10
MARCO TEÓRICO		10
2.1	Voz sobre IP.....	10
2.2	Protocolo SIP.....	11
2.3	Protocolo IAX2.....	12
2.4	Asterisk.....	13
CAPÍTULO 3.....		15
ANÁLISIS DE INFRAESTRUCTURA		15
3.1	Identificación de terminales	15
3.1.1	Teléfonos basados en hardware	15
3.1.2	Teléfonos basados en software	17
3.2	Identificación de equipos de comunicaciones.....	20
3.3	Identificación de centrales telefónicas	22
3.4	Arquitectura de comunicaciones del call center.....	23
3.5	Protocolos de comunicación del call center.....	25
CAPÍTULO 4.....		27

DISEÑO E IDENTIFICACIÓN DE VULNERABILIDADES	27
4.1 Diseño de pruebas de identificación de vulnerabilidades	27
4.2 Escenario.....	28
4.3 Ataques de reconocimiento	30
4.2.1 Reconocimiento de versiones	30
4.2.2 Reconocimiento de puertos y servicios.....	31
4.2.3 Reconocimiento de extensiones	35
4.4 Ataques de interceptación	37
4.5 Ataques de denegación de servicios	39
4.6 Ataques por Fuerza Bruta.....	44
4.7 Explotación de Vulnerabilidades.....	47
CAPÍTULO 5.....	49
IMPLEMENTACIÓN DE SOLUCIONES DE SEGURIDAD INFORMÁTICA ...	49
5.1 Actualización del sistema	49
5.2 Cifrado en las comunicaciones de VoIP	52
5.3 Listas de control de acceso	58
5.4 Políticas de contraseñas	60
5.5 Seguridad perimetral	60

5.6 Implementación del IPS.....	62
CAPÍTULO 6.....	65
PRUEBAS DE LA SEGURIDAD INFORMÁTICA APLICADA.....	65
6.1 Validación del cifrado en las comunicaciones de VoIP.....	65
6.2 Validación de la seguridad informática en las ACL's.....	69
6.3 Validación de la seguridad informática en ataques de fuerza bruta ..	71
6.4 Validación de la seguridad informática en ataques de denegación de servicios	73
CONCLUSIONES Y RECOMENDACIONES.....	77
BIBLIOGRAFÍA.....	80
ANEXOS.....	2

ABREVIATURAS Y SIMBOLOGÍA

ACL	(Access Control List) Lista de control de acceso.
ARP	(Address Resolution Protocol) Protocolo de resolución de direcciones.
CLI	(Command Line Interface) Registro detallado de llamada.
CDR	(Call Detail Record) Registro detallado de llamada.
DHCP	(Dynamic Host Configuration Protocol) Protocolo de configuración dinámica de host.
DTLS	(Datagram Transport Layer Security) Seguridad de la capa de transporte en datagrama.
IAX2	(Inter-Asterisk eXchange protocol) Protocolo de intercambio entre Asterisk versión 2.
IDS	(Intrusion Detection System) Sistema de detección de intrusos.
IP	(Internet Protocol) Protocolo de internet.
IPS	(Intrusion Prevention System) Sistema de prevención de intrusos.
IPsec	(Internet Protocol security) Seguridad en el protocolo de internet.

PBX	(Private Branch Exchange) Central secundaria privada.
SIP	(Session Initiation Protocol) Protocolo de inicio de sesión.
SRTP	(Secure Real-time Transport Protocol) Protocolo seguro de transporte en tiempo real.
TCP	(Transmission Control Protocol) Protocolo de control de transmisión.
TLS	(Transport Layer Security) Seguridad de la capa de transporte.
UDP	(User Datagram Protocol) Protocolo de datagrama de usuario.
VoIP	(Voice over IP) Voz sobre IP.
VPN	(Virtual Private Network) Red privada virtual.
WAP	(Wireless Access Point) Punto de acceso inalámbrico.

GLOSARIO

ATAQUE INFORMÁTICO.- Es un método por el cual una o varias personas intentan causar problemas, daños o robos de información en un sistema informático.

CALL CENTER.- Conocido como el centro de llamadas telefónicas, es un área donde labora personal especialmente entrenado para realizar y recibir llamadas de clientes, afiliados, compañías, que buscan ser atendidos por un servicio en particular.

CERTIFICADO DIGITAL.- Es un archivo digital generado por una autoridad de certificación que asocia información de identidad de un usuario u organización, mediante este certificado digital se validará la identidad digital de un usuario, además, es utilizado para cifrar la información de una comunicación y firmar digitalmente documentos.

DISTRIBUCIÓN LINUX.- Es una recopilación de software dedicado a un fin específico para satisfacer las necesidades de un grupo de usuarios, este conjunto de software opera bajo el sistema operativo Linux.

ENVENENAMIENTO ARP.- Es una técnica de ataque informático, generalmente utilizada por las amenazas para espiar el tráfico que fluye en una red de datos y de esta manera poder obtener información hacia su propia tarjeta de red consiguiendo datos sensibles.

EXTENSIONES TELEFÓNICAS.- Las extensiones telefónicas son las ramificaciones de la central telefónica, también conocidas como anexos telefónicos, generalmente son un teléfono desde donde el personal de la organización puede realizar y recibir llamadas telefónicas.

HACKING ETICO.- Es la aplicación de los conocimientos de informática y seguridad que tienen los especialistas informáticos para realizar un análisis de vulnerabilidades a una infraestructura informática o a una red de datos, generando un informe con los hallazgos encontrados y sugiriendo medidas de seguridad que se pueden aplicar para solventar estas debilidades.

OPERADORES DE CALL CENTER.- Es el personal que labora en el call center atendiendo las llamadas de los clientes, atendiendo sus requerimientos de solicitud de servicios.

PROTOCOLOS DE SEÑALIZACIÓN.- Son el conjunto de normas y procedimientos que definen los mecanismos que se emplearán en la transmisión de la voz, transformándolos en paquetes de datos que serán transmitidos a través de una red de datos.

VECTORES DE ATAQUES.- Un vector de ataque es el método que utiliza un atacante para llevar a cabo su ataque informático hacia su objetivo en particular.

TÚNELES IP.- Los túneles **IP** se refiere al encapsulamiento de un protocolo de red sobre otro generando un conducto de información, los túneles **IP** generalmente son cifrados cuando son utilizados en una **VPN**.

WIRELESS ACCESS POINT.- El Wireless Access Point (WAP) es un dispositivo de red que permite conectarse inalámbricamente a una red de datos. Los dispositivos móviles tales como laptops, celulares, tabletas, generalmente utilizan este medio para conectarse a redes de datos para obtener acceso al Internet.

ÍNDICE DE FIGURAS

Figura 1.1 Diagrama de interconexión del call center con la red telefónica	2
Figura 1.2 Diagrama de interconexión telefónica entre las distintas filiales	3
Figura 1.3 Diagrama de una infraestructura de comunicaciones de VoIP encriptada	6
Figura 1.4 Diagrama de una infraestructura de comunicaciones de VoIP utilizando túneles VPN.....	7
Figura 3.1 Teléfono basado en hardware Polycom SoundPoint IP 331	17
Figura 3.2 Teléfono basado en software X-Lite 3.0	19
Figura 3.3 Conmutador Cisco Catalyst 2960-X.....	21
Figura 3.4 Conmutador Cisco Catalyst 3750-X.....	22
Figura 3.5 Servidor HP Proliant DL 380p G8	23
Figura 3.6 Arquitectura de comunicaciones del call center.....	25
Figura 4.1 Diseño de pruebas de identificación de vulnerabilidades	28
Figura 4.2 Escenario para el despliegue de los vectores de ataques	30
Figura 4.3 Reconocimiento de versiones del software de la central telefónica “192.168.1.7”	31
Figura 4.4 Reconocimiento de versiones del software de la central telefónica “192.168.4.230”	31

Figura 4.5 Escaneo de puertos a la central telefónica “192.168.1.7”	32
Figura 4.6 Escaneo de puertos a la central telefónica “192.168.4.230”	33
Figura 4.7 Módulo de FreePBX en la central telefónica “192.168.1.7”	35
Figura 4.8 Módulo de FreePBX en la central telefónica “192.168.4.230”	35
Figura 4.9 Reconocimiento de extensiones en la central telefónica “192.168.1.7”	36
Figura 4.10 Reconocimiento de extensiones en la central telefónica “192.168.4.230”	37
Figura 4.11 Envenenamiento ARP con la herramienta “ettercap”	38
Figura 4.12 Captura de paquetes en las comunicaciones de VoIP y reproducción de audio de las conversaciones del personal de la organización.	39
Figura 4.13 Ataque de denegación de servicio a la central telefónica “192.168.1.7”	40
Figura 4.14 Ataque de denegación de servicio a la central telefónica “192.168.4.230”	40
Figura 4.15 CLI de la central telefónica “192.168.1.7” mostrando el ataque de denegación de servicios	41
Figura 4.16 CLI de la central telefónica “192.168.4.230” mostrando el ataque de denegación de servicios	42

Figura 4.17 Carga promedio de la central telefónica “192.168.1.7”, durante el ataque de denegación de servicios.....	43
Figura 4.18 Carga promedio de la central telefónica “192.168.4.230”, durante el ataque de denegación de servicios.....	43
Figura 4.19 Estado de los teléfonos durante el ataque de denegación de servicios.....	44
Figura 4.20 Generación del diccionario de claves numéricas.....	45
Figura 4.21 Ataque de fuerza bruta basada en diccionario a la extensión “101” de la central “192.168.4.230”.....	46
Figura 4.22 Ataque de fuerza bruta basada en diccionario a la extensión “500” de la central “192.168.4.230”.....	46
Figura 4.23 Autenticación a la central telefónica “192.168.4.230” desde la máquina atacante	47
Figura 4.24 Autenticación exitosa en la central “192.168.4.230” y generación de llamadas telefónicas desde la máquina atacante.....	48
Figura 5.1 Versión actualizada de “Asterisk” en la central telefónica “192.168.4.230”.....	50
Figura 5.2 Versión actualizada de “FreePBX” en la central telefónica “192.168.4.230”.....	51

Figura 5.3 Creación de la autoridad certificadora en la central telefónica “192.168.4.230”	53
Figura 5.4 Emisión de certificado para la central telefónica “192.168.4.230”	53
Figura 5.5 Emisión de certificado para la extensión “500” de la central telefónica “192.168.4.230”	54
Figura 5.6 Certificados digitales almacenados en la central telefónica “192.168.4.230”	54
Figura 5.7 Configuraciones avanzadas del protocolo SIP para la habilitación del cifrado en las comunicaciones de VoIP con el protocolo TLS	55
Figura 5.8 Configuración del protocolo TLS y SRTP en la extensión telefónica “500” de la central telefónica “192.168.4.230”	56
Figura 5.9 Configuración del protocolo DTLS para la extensión “500” de la central telefónica “192.168.4.230”	56
Figura 5.10 Configuración del cifrado de las comunicaciones de VoIP en el archivo “sip.conf” de la extensión “500” en la central telefónica “192.168.4.230”	57
Figura 5.11 Configuración de la ACL en la extensión “500” de la central telefónica “192.168.4.230”	58
Figura 5.12 Configuración de la ACL en el archivo “sip.conf” para la extensión “500” de la central telefónica “192.168.4.230”	59

Figura 5.13 Contraseña generada por la aplicación “FreePBX” en la creación de una extensión.....	60
Figura 5. 14 Configuración de los parámetros criptográficos de la VPN IPsec..	62
Figura 5.15 Conexión VPN entre las filiales de Guayaquil y México.....	62
Figura 5.16 Políticas de configuración de la aplicación “Fail2ban”	63
Figura 5.17 Perfil de filtrado del Fail2ban para análisis de logs de la aplicación “Asterisk”	64
Figura 5. 18 Perfil de filtrado del Fail2ban para análisis de logs de la aplicación “Asterisk”	64
Figura 6.1 Configuración de la cuenta SIP en la aplicación “Zoiper”	66
Figura 6.2 Configuración del certificado digital y protocolos de comunicaciones seguras en la aplicación “Zoiper”	67
Figura 6.3 Configuración del certificado digital de la autoridad de certificación en la aplicación “Zoiper”	68
Figura 6.4 Autenticación exitosa a la central telefónica “192.168.4.230” de la extensión telefónica “700”	68
Figura 6.5 Validación del cifrado de las comunicaciones de VoIP por parte de los protocolos de comunicaciones seguras	69
Figura 6.6 Estado de prohibido luego de tratar la autenticación SIP de la extensión “500”	70

Figura 6.7 Registros de logs de la central telefónica “192.168.4.230” mostrando la efectividad de la ACL	70
Figura 6.8 Despliegue del ataque de fuerza bruta basado en un diccionario de claves aplicado a la extensión “500” de la central telefónica “192.168.4.230”	71
Figura 6.9 Errores durante la ejecución del ataque de fuerza bruta a la central telefónica “192.168.4.230”	72
Figura 6.10 Log de “Asterisk” evidenciando los intentos de autenticación a la extensión “500” de la central telefónica “192.168.4.230”	72
Figura 6.11 Log de “Fail2ban evidenciando el bloqueo aplicado a la dirección IP “192.168.4.128”	73
Figura 6.12 Ejecución del ataque de denegación de servicios sobre la central telefónica “192.168.4.230” utilizando la extensión “500”	74
Figura 6.13 Log de “Fail2ban evidenciando el bloqueo aplicado a la dirección IP “192.168.4.128”	74

ÍNDICE DE TABLAS

Tabla 1 Características técnicas del teléfono basado en hardware Polycom SoundPoint IP 331	17
Tabla 2 Características técnicas del teléfono basado en software X-Lite 3.0	18
Tabla 3 Características técnicas del conmutador Cisco Catalyst 2960-X	20
Tabla 4 Características técnicas del conmutador Cisco Catalyst 3750-X	21
Tabla 5 Características técnicas del servidor HP Proliant DL 380p G8	22
Tabla 6 Puertos bien conocidos encontrados durante el escaneo de puertos...	33

INTRODUCCIÓN

Hace algunos años, las empresas dedicadas al negocio de call center tenían en su infraestructura tecnológica centrales telefónicas análogas y análogas-digitales dedicadas a brindar el servicio de comunicaciones, las estaciones de trabajo del personal contaban con su propio cableado telefónico desde el teléfono hacia la central telefónica, este cableado era independiente del cableado de la red de datos, además, las centrales contaban con un licenciamiento por canales de voz, lo cual representaba una gran inversión para las compañías.

Con el auge de la telefonía sobre la red de datos, más conocida como **VoIP**, surgió como una alternativa ante estos inconvenientes a los que se enfrentaban las organizaciones. Implementaciones basadas en software libre como “Asterisk”, se hacen popular por su uso e implementación en las organizaciones, ahora pueden utilizar la misma red de datos para la transmisión de voz, reduciendo considerablemente la inversión que hacían las organizaciones en licenciamiento y cableado estructurado, inclusive el teléfono físico puede ser sustituido por una aplicación instalada en el computador que maneje los protocolos de señalización de **VoIP** y el auricular del teléfono es remplazado por unos audífonos con micrófono conectados al computador.

Sin embargo, el mismo hecho de que la transmisión de la voz se la realiza a través de la red de datos, ha despertado el interés en los atacantes para elaborar herramientas y procedimientos con la finalidad de vulnerar la seguridad en las comunicaciones, por consiguiente, han obteniendo provecho de estas debilidades, generando beneficios económicos para ellos mismos promocionando llamadas gratuitas ilimitadas o inclusive originando indisponibilidad en los servicios de comunicaciones, que a su vez ocasionan daños y perjuicios a las organizaciones.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

La compañía MEDIASIST S.A ha 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 Telemarketing.
- 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.

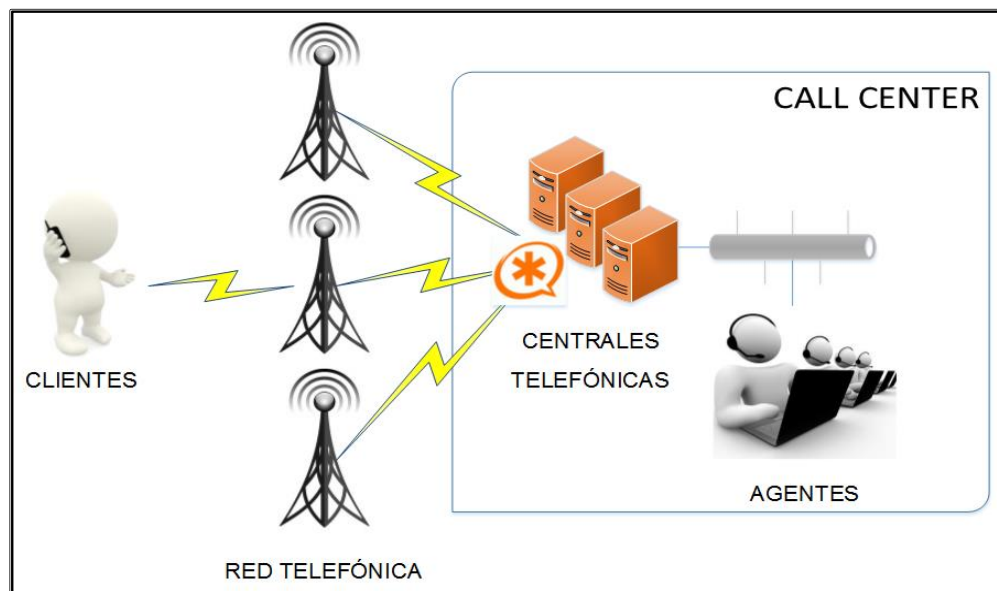


Figura 1.1 Diagrama de interconexión del call center con la red telefónica

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.

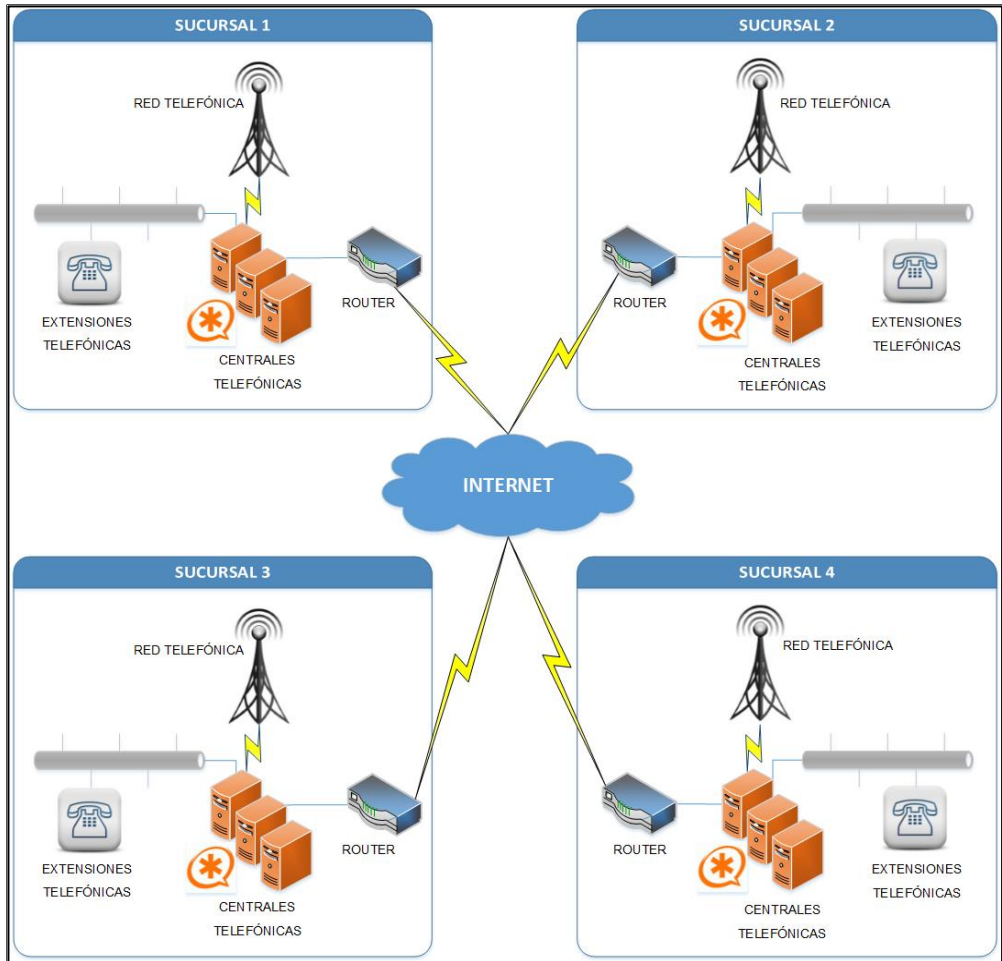


Figura 1.2 Diagrama de interconexión telefónica entre las distintas filiales

1.2 Descripción del problema

Una vez presentados los antecedentes de la infraestructura de comunicaciones de **VoIP** sobre la cual opera la organización, se describirán los problemas informáticos de los cuales ha sido víctima la organización.

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.

1.3 Solución propuesta

Con la finalidad de mitigar los problemas generados por los ataques informáticos en las comunicaciones telefónicas, se procederá a

implementar las siguientes medidas de seguridad informática en la infraestructura de la organización:

Cifrado en las comunicaciones de VoIP. Esto se logrará a través del cifrado de los protocolos **SIP** y **RTP** que utilizan las centrales telefónicas para las comunicaciones de **VoIP** en la organización. Ahora las comunicaciones serán cifradas por los protocolos **SIP** sobre **TLS** y **SRTP** que brindan una protección sobre las amenazas que intentan espiar las conversaciones telefónicas de los usuarios en la organización.

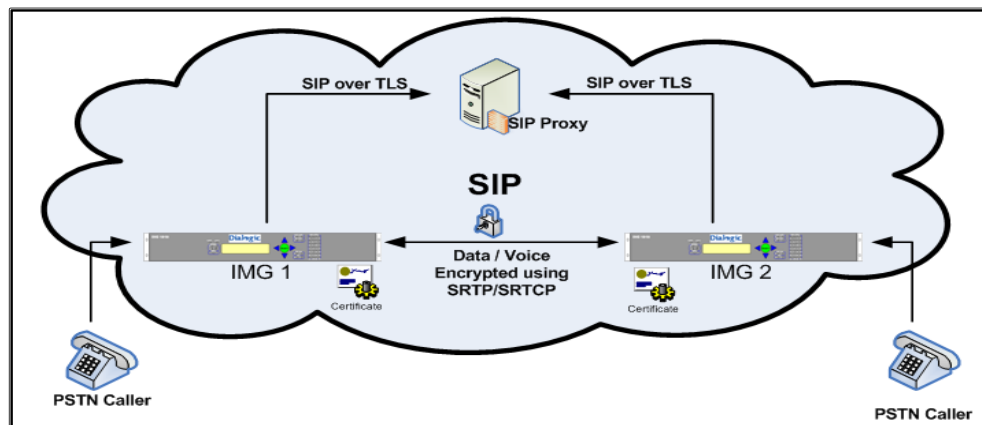


Figura 1.3 Diagrama de una infraestructura de comunicaciones de VoIP encriptada

Listas de control de acceso para las extensiones telefónicas. Se crearán listas de control de acceso en las extensiones que utilizan los operadores, es decir, cada extensión podrá ser utilizada desde el equipo que disponga la lista de acceso y no podrá ser utilizada en cualquier dispositivo para un uso fraudulento.

Implementación de seguridad perimetral. Se implementarán túneles **VPN**, en donde la comunicación entre las sucursales será cifrada con algoritmos de encriptación utilizando como medio de comunicación el Internet.

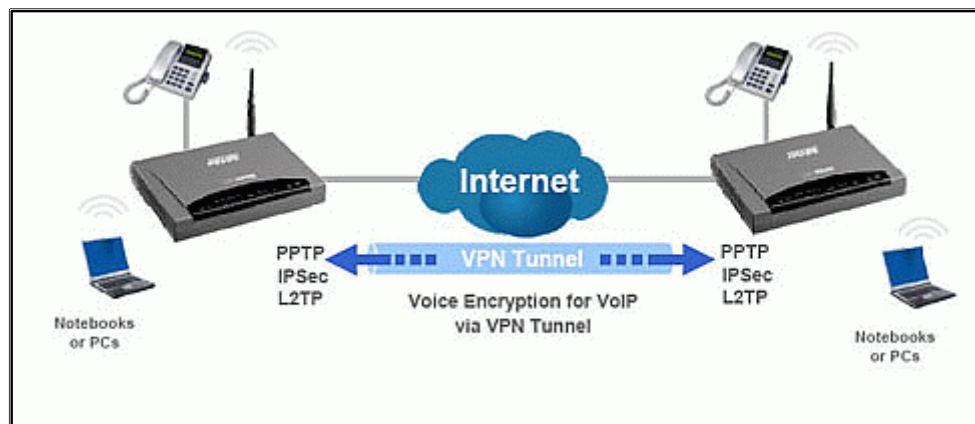


Figura 1.4 Diagrama de una infraestructura de comunicaciones de VoIP utilizando túneles VPN

Implementación de IPS en las centrales telefónicas. Se implementará un **IPS** para evitar ataques por fuerza bruta. Esta aplicación analizará los registros de intentos de ataques y bloqueará selectivamente la dirección **IP** origen de estos ataques.

1.4 Objetivos generales

Realizar un análisis de vulnerabilidades informáticas a la infraestructura de comunicaciones de **VoIP** de la empresa MEDIASIST S.A, esto es, con la finalidad de encontrar las debilidades a las que se encuentra expuesta la infraestructura de comunicaciones telefónicas.

Proponer e implementar medidas de seguridad informática orientadas a la infraestructura de comunicaciones de **VoIP**, esto es, con el objetivo de mitigar el riesgo informático al que se enfrenta la organización.

1.5 Objetivos específicos

Para alcanzar los objetivos generales, se llevará a cabo los siguientes objetivos específicos:

- Describir los conceptos de seguridad referentes a las comunicaciones de **VoIP**.
- Identificar los elementos tecnológicos que intervienen en las comunicaciones de **VoIP**.
- Realizar un análisis de vulnerabilidades a los elementos que intervienen en las comunicaciones de **VoIP**.
- Implementar mecanismos de seguridad en las de comunicaciones de **VoIP**, por consiguiente, se pretende mitigar las debilidades encontradas en el análisis de vulnerabilidades realizado.
- Realizar pruebas de seguridad informática para validar los mecanismos implementados en la infraestructura de comunicaciones de **VoIP**.

1.6 Metodología

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

CAPÍTULO 2

MARCO TEÓRICO

2.1 Voz sobre IP

Roberto Gutiérrez Gil define la **VoIP** como una tecnología soportada en una infraestructura de red de datos, resalta el proceso de transmisión de la voz y hace énfasis en las características técnicas de la tecnología [1].

VoIP es el acrónimo de “Voice Over Internet Protocol”, que tal y como el término dice, hace referencia a la emisión de voz en paquetes IP sobre redes de datos como puede ser Internet. Llegados a este punto se unen dos mundos que hasta entonces habían convivido separados: la transmisión de voz y la de datos [1].

La tecnología VoIP trata de transportar la voz, previamente procesada, encapsulándola en paquetes para poder ser

transportadas sobre redes de datos sin necesidad de disponer de una infraestructura telefónica convencional. Con lo que se consigue desarrollar una única red homogénea en la que se envía todo tipo de información ya sea voz, video o datos [1].

Elvira Misfud Talón y Raúl V. Lerma-Blasco destacan el uso y aprovechamiento de las funcionalidades que brinda la **VoIP** en la actualidad [2].

El auge de las comunicaciones a través de IP es evidente. Hoy en día pueden distribuirse a través de la red y en tiempo real mensajes escritos o que incorporen voz e imágenes en forma de paquetes de información. La tecnología VoIP, de acuerdo con la definición establecida en 1996 por la Unión Internacional de Telecomunicaciones (UIT), permite la fusión de dos elementos hasta entonces separados: la voz y los datos. De este modo, pueden aprovecharse mejor los recursos que ofrece Internet para disminuir el coste de las llamadas y el de los servicios multimedia [2].

2.2 Protocolo SIP

José L. Villalón describe las características del protocolo de control y señalización **SIP**, utilizado en **VoIP**; además, el autor menciona las solicitudes y respuestas que intervienen en el proceso de comunicación [3].

SIP (Session Initiation Protocol) es un protocolo de control desarrollado por el IETF, basado en arquitectura cliente/servidor similar al HTTP, legible por humanos, con el que comparte muchos códigos de estado y sigue una estructura de petición-respuesta; estas peticiones son generadas por un cliente y enviadas a un servidor, que las procesa y devuelve la respuesta al cliente. El par petición-respuesta recibe el nombre de transacción. Al igual que el protocolo HTTP, SIP proporciona un conjunto de solicitudes y respuestas basadas en códigos [3].

El protocolo SIP define principalmente seis tipos de solicitudes:

INVITE: establece una sesión.

ACK: confirma una solicitud INVITE.

BYE: finaliza una sesión.

CANCEL: cancela el establecimiento de una sesión.

REGISTER: comunica la localización de usuario (nombre de equipo, IP).

OPTIONS: comunica la información acerca de las capacidades de envío y recepción de teléfonos SIP.

2.3 Protocolo IAX2

El portal de Elastix Tech menciona las características del protocolo IAX en su versión **IAX2**, describiendo su funcionalidad y utilidad [4].

IAX (*Inter-Asterisk eXchange protocol*) es uno de los protocolos utilizado por Asterisk. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre

servidores y clientes que también utilizan protocolo IAX. El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX. El protocolo original ha quedado obsoleto en favor de IAX2 [4].

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de *códecs* y un gran número de *streams*, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas. ESTA DISEÑADO PARA DARLE PRIORIDAD A LOS PAQUETES DE VOZ SOBRE UNA RED IP [4].

2.4 Asterisk

Elvira Misfud Talón y Raúl V. Lerma-Blasco describen los inicios del software de telefonía IP Asterisk, su evolución, uso y distribución; además, se destacan las características técnicas que tiene el software [2].

Asterisk es un proyecto de código abierto que permite disponer de una centralita software y, al mismo tiempo, de un sistema interactivo de voz. Creado en un principio por Mark Spencer, posteriormente lo liberó y lo distribuyó bajo licencia GNU/GPL (aunque también existen licencias comerciales). Escrito en C, se creó para GNU/Linux, si bien hoy existen versiones para Unix, Mac OS X y Windows, entre otros [4].

Sus principales características son las siguientes:

- **Soporta telefonía tradicional: líneas analógicas RTC/RTB (PSTN/POTS), líneas digitales RDSI (E1, T1, accesos básicos, accesos primarios), etcétera.**
- **Establece un puente transparente entre diferentes protocolos VoIP: SIP, H.323, IAX/IAX2, etcétera.**
- **Crea también un puente transparente entre diferentes tecnologías: RTC/RTB, RDSI, GSM, etcétera.**
- **Dispone de un API independiente del hardware.**
- **Posee una interfaz de comunicación con aplicaciones.**

CAPÍTULO 3

ANÁLISIS DE INFRAESTRUCTURA

3.1 Identificación de terminales

Las extensiones telefónicas son creadas como cuentas **SIP** en las centrales telefónicas y han sido configuradas en dos clases de teléfonos. El primer tipo de teléfono está basado en hardware y el segundo tipo está basado en software.

3.1.1 Teléfonos basados en hardware

El portal de la compañía 3CX describe las características de un teléfono basado en hardware como un dispositivo que opera similar a un teléfono convencional con la característica de compartir la red de datos con el computador [5].

Un teléfono SIP basado en hardware tiene la apariencia de un “teléfono” normal y actúa como tal. Sin embargo, se conecta directamente a la red de datos. Estos teléfonos tienen un miniconcentrador integrado para que puedan compartir la conexión de red con el ordenador. De esa forma, no se necesita un punto de red adicional para el teléfono [5].

Los teléfonos basados en hardware están ubicados en los escritorios de trabajo del personal administrativo para realizar y recibir llamadas inherentes a sus actividades de gestión; también los teléfonos se encuentran en las estaciones de los operadores del departamento de operaciones, donde se encargan de recibir las llamadas de emergencias de los afiliados.

Con el objetivo de abastecer la demanda de teléfonos requeridos por el departamento de operaciones y el personal administrativo, el departamento de sistemas ha adquirido una gama de teléfonos basados en hardware que soportan el protocolo de señalización **SIP**, estos dispositivos son fabricado por la compañía “Polycom” y tienen las características que se muestran en la siguiente tabla:

Tabla 1 Características técnicas del teléfono basado en hardware Polycom SoundPoint IP 331

Característica	Descripción
Fabricante	Polycom
Modelo	SoundPoint IP 331
Líneas	Capacidad para dos líneas SIP
Puertos Ethernet	2 puertos 10/100 Mbps
Codecs soportados	G.711 u/A and G.729 ^a



Figura 3.1 Teléfono basado en hardware Polycom SoundPoint IP 331

3.1.2 Teléfonos basados en software

La compañía 3CX en su página web describe al teléfono basado en software como una aplicación que puede ser instalada en los ordenadores, este aplicativo tiene la capacidad

de conectarse a una central telefónica y realizar llamadas utilizando los audífonos o altavoces del computador [5].

Un teléfono SIP basado en software, es un programa que utiliza el micrófono y los altavoces de su ordenador, o auriculares conectados, para permitirle realizar o recibir llamadas [5].

En la organización, los teléfonos basados en software son instalados en los computadores de los operadores de telemarketing que realizan la venta de servicios mediante llamadas telefónicas. En los ordenadores se encuentra instalado la aplicación “X-Lite”, el cual es un teléfono basado en software con la capacidad de tener configurada una cuenta **SIP**. Los operadores utilizan audífonos con micrófono para interactuar con el teléfono durante la llamada telefónica, el software tiene las siguientes características:

Tabla 2 Características técnicas del teléfono basado en software X-Lite 3.0

Característica	Descripción
Fabricante	Counterpath
Versión	3.0

Líneas	Capacidad para una líneas SIP
Video	Soporte para video
Codecs de audio soportados	G.711 u/A, GSM, Broadvoice-32, entre otros.
Codecs de video soportados	H.263
Audio	Calidad de Servicio en el audio



Figura 3.2 Teléfono basado en software X-Lite 3.0

3.2 Identificación de equipos de comunicaciones

La comunicación entre los teléfonos basados en hardware/software y las centrales telefónicas está dada por una red de datos. La infraestructura de la red de datos está compuesta por un cableado estructurado de categoría 6A, en donde cada estación de trabajo cuenta con un punto de acceso a la red de datos.

Los puntos de datos están interconectados a través de conmutadores de capa 2, donde cada puerto está configurado para tener una velocidad de transferencia a 1 Gbps. Los diferentes conmutadores se encuentran interconectados en forma de cascada. El departamento de sistemas ha adquirido conmutadores del fabricante Cisco que tiene las siguientes características:

Tabla 3 Características técnicas del conmutador Cisco Catalyst 2960-X

Característica	Descripción
Fabricante	Cisco
Modelo	Catalyst 2960-X
Puertos	24 o 48 Fast Ethernet
Velocidad Enlace	Gigabit Ethernet



Figura 3.3 Conmutador Cisco Catalyst 2960-X

Con el objetivo de establecer la comunicación entre los diferentes segmentos de red de las localidades de Quito y Guayaquil, se han adquirido conmutadores de capa 3 que incluyen la característica de enrutamiento. Estos conmutadores son del fabricante Cisco, el cual cuenta con las siguientes características:

Tabla 4 Características técnicas del conmutador Cisco Catalyst 3750-X

Característica	Descripción
Fabricante	Cisco
Modelo	Catalyst 3750-X
Puertos	24 o 48 Fast Ethernet
Velocidad Enlace	Gigabit Ethernet
Enrutamiento	Capacidad para administrar

	protocolos de enrutamiento.
--	-----------------------------



Figura 3.4 Conmutador Cisco Catalyst 3750-X

3.3 Identificación de centrales telefónicas

Las centrales telefónicas contienen una solución basada en software libre que se encuentra instalada en servidores de rack que tienen las siguientes características:

Tabla 5 Características técnicas del servidor HP Proliant DL 380p G8

Característica	Descripción
Fabricante	HP
Modelo	Proliant DL 380p G8
Procesador	Intel Xeon E5-2630 de 6 núcleos
Memoria RAM	8 GB
Disco Duro	600 GB RAID 0
Fuentes de Poder	Redundantes

Velocidad de Enlace	10/100/1000 Mbps
----------------------------	------------------



Figura 3.5 Servidor HP ProLiant DL 380p G8

3.4 Arquitectura de comunicaciones del call center

La arquitectura de comunicaciones del call center está conformada por los elementos tecnológicos previamente descritos, tales como: las terminales con teléfonos basados en hardware/software, los conmutadores y los servidores de las centrales telefónicas.

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.

Con la finalidad de realizar el análisis de vulnerabilidades a la infraestructura de comunicaciones de **VoIP**, la organización nos ha

proporcionado como información técnica la cantidad de centrales telefónicas que posee. 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.

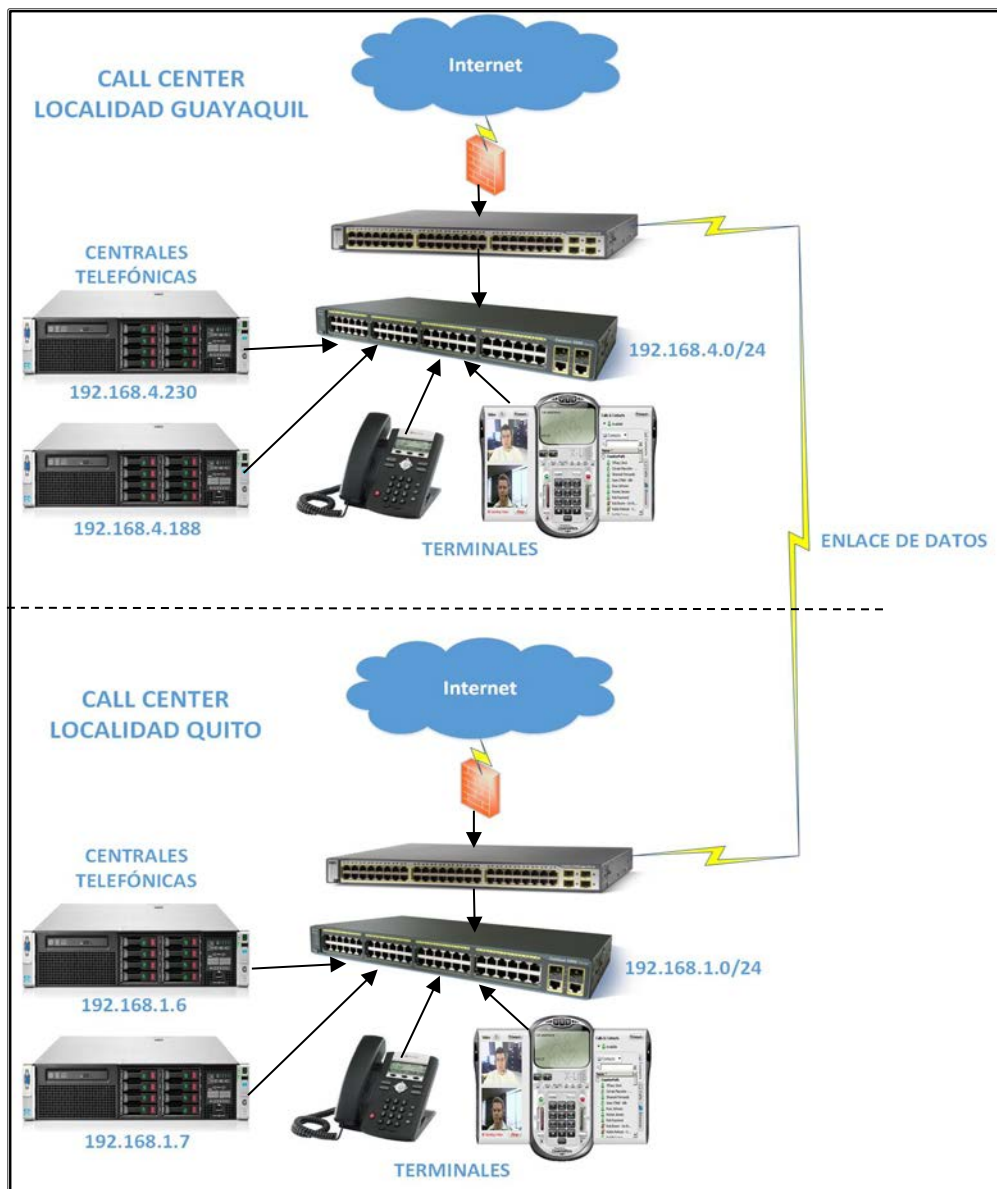


Figura 3.6 Arquitectura de comunicaciones del call center

3.5 Protocolos de comunicación del call center

Como política de implementación y configuración de interconexiones en centrales telefónicas, el departamento de sistemas ha establecido que: La selección del protocolo de comunicación a utilizar depende de

la localidad donde se encuentren las centrales telefónicas que van a ser interconectadas. Si las centrales se encuentran dentro del mismo segmento de Red o se encuentran alojadas en diferentes localidades que pertenecen al mismo país (ejemplo: Quito-Guayaquil), entonces el protocolo que se utilizará es **SIP** formando una troncal **SIP**. En el caso de que las centrales telefónicas a interconectar se encuentren en distintas localidades pertenecientes a diferentes países (ejemplo: Guayaquil - México D.F), entonces el protocolo que se utilizará es **IAX2** formando una troncal **IAX2**.

Desde las terminales que tienen teléfonos basados en hardware/software hacia las centrales telefónicas se utiliza exclusivamente el protocolo de comunicaciones **SIP**.

CAPÍTULO 4

DISEÑO E IDENTIFICACIÓN DE VULNERABILIDADES

4.1 Diseño de pruebas de 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 4.1 Diseño de pruebas de identificación de vulnerabilidades

El diseño presentado en la Figura 4.1 está basado en la metodología de hacking ético planteada para el desarrollo del presente trabajo de análisis de vulnerabilidades, por consiguiente, se han seleccionado los siguientes vectores de ataques que se desplegarán hacia el objetivo:

- Ataques de Reconocimiento
- Ataques de Intercepción
- Ataques de Denegación de Servicios
- Ataques por Fuerza Bruta
- Explotación de Vulnerabilidades

4.2 Escenario

Con la finalidad de desplegar los vectores de ataques estructurados sobre la infraestructura de comunicaciones telefónicas de la organización, se incorporará un computador a la red de datos de la

organización en la localidad de Guayaquil, además, este computador se conectará a la red de datos mediante acceso inalámbrico.

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.

El **WAP** permitirá el acceso inalámbrico al computador atacante a la red de datos y tiene la dirección **IP**: 192.168.4.128, además, mediante el protocolo **DHCP** distribuye direcciones **IP** del segmento de red 192.168.184.0/24 a los equipos que se conecten. La computadora atacante tiene asignada la dirección **IP**: 192.168.184.13 y desde esta conexión inalámbrica se tiene acceso a todas las centrales de la organización, incluyendo las de la localidad de Quito.

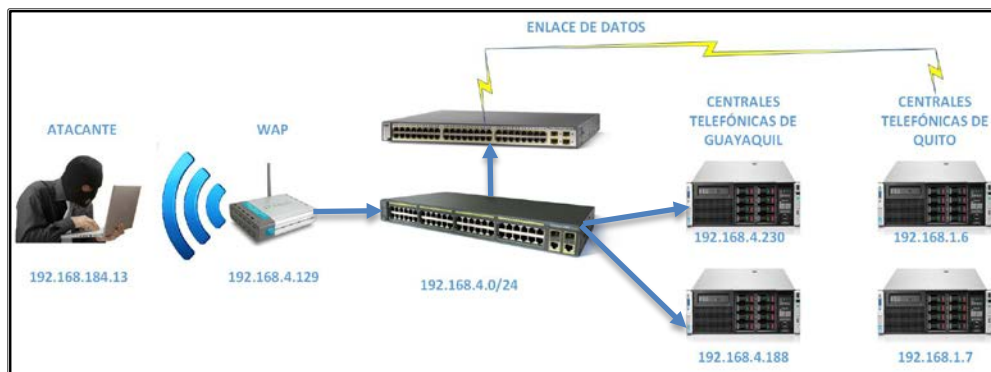


Figura 4.2 Escenario para el despliegue de los vectores de ataques

4.3 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.

4.2.1 Reconocimiento de versiones

En un principio, la información que se pretende conseguir es referente al software que tiene instalado la central telefónica. Se busca conocer las características de la aplicación que tiene instalada la central y posteriormente utilizar las herramientas apropiadas que nos permitan realizar un análisis de vulnerabilidades a su seguridad informática.

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:~# svmmap 192.168.1.7 -m INVITE
| SIP Device          | User Agent              | Fingerprint |
|-----|-----|-----|
| 192.168.1.7:5060    | Asterisk PBX 1.6.2.20  | disabled    |

```

Figura 4.3 Reconocimiento de versiones del software de la central telefónica “192.168.1.7”

```

root@kali:~# svmmap 192.168.4.230 -m INVITE
| SIP Device          | User Agent              | Fingerprint |
|-----|-----|-----|
| 192.168.4.230:5060 | Asterisk PBX 1.6.0.6-rc1 | disabled    |

```

Figura 4.4 Reconocimiento de versiones del software de la central telefónica “192.168.4.230”

4.2.2 Reconocimiento de puertos y servicios

Continuando con la fase de recopilación de información, se realizará un escaneo de puertos y servicios que se encuentran

habilitados en los servidores de las centrales telefónicas de la infraestructura de comunicaciones de **VoIP**.

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

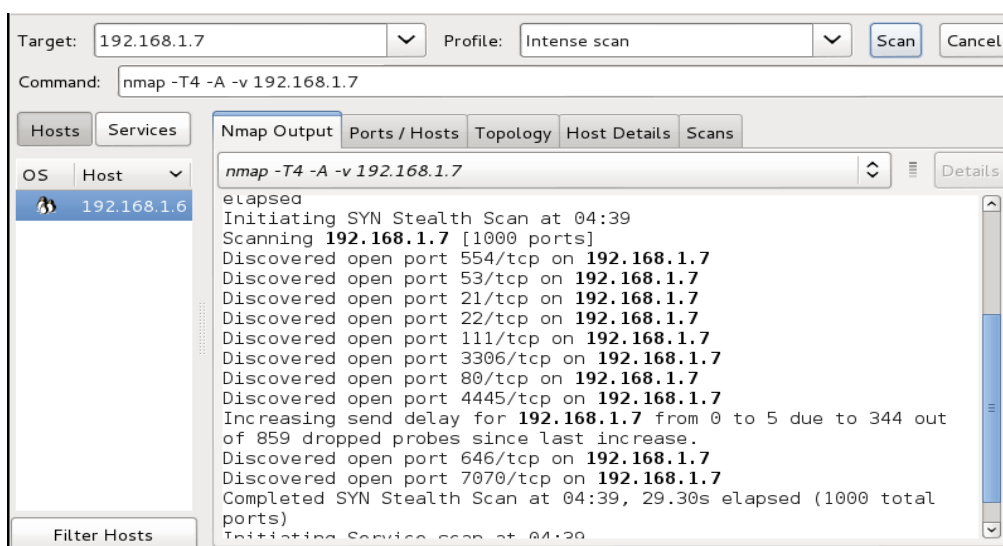


Figura 4.5 Escaneo de puertos a la central telefónica “192.168.1.7”

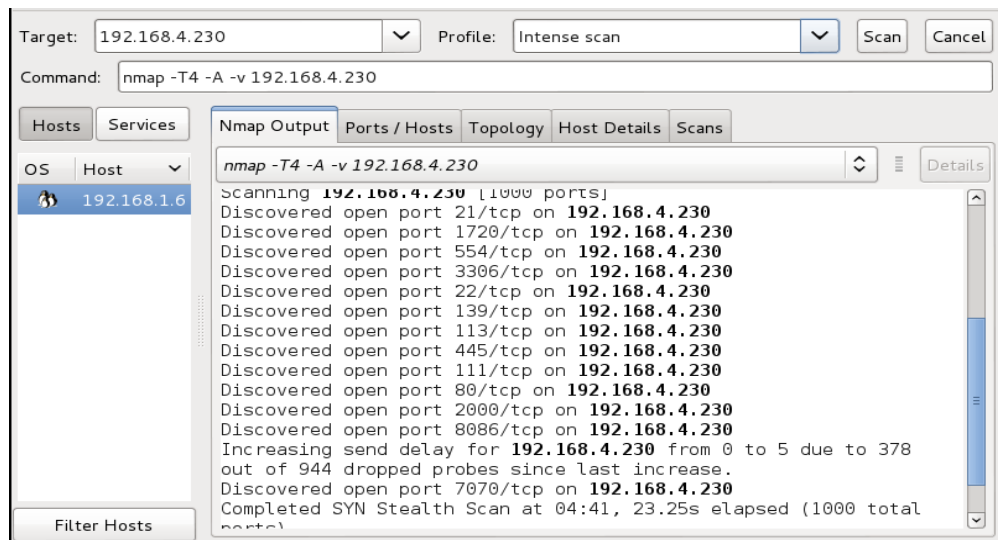


Figura 4.6 Escaneo de puertos a la central telefónica “192.168.4.230”

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

Tabla 6 Puertos bien conocidos encontrados durante el escaneo de puertos

Puerto (TCP)	Descripción
21	FTP
22	SSH, SFTP, SCP
53	DNS
80	HTTP

111	SunRPC
113	Ident
139	NetBIOS
554	RTSP
3306	MYSQL

En la Tabla 6 podemos apreciar servicios bien conocidos como: un servicio de aplicaciones web “Apache” y una base de datos “MYSQL”. El encontrar estos servicios nos da una pauta de que existen componentes adicionales al software de la central telefónica, para ello se accede mediante un navegador web a las direcciones **IP** de las centrales telefónicas de la organización y se determina que las centrales telefónicas “Asterisk” tienen instalado un módulo de administración de las configuraciones denominado “FreePBX” en sus versiones “2.5” y “2.7”, este módulo es una aplicación web que utiliza el servidor web “Apache” y la base de datos “MYSQL” como un repositorio para almacenar la información de las configuraciones.

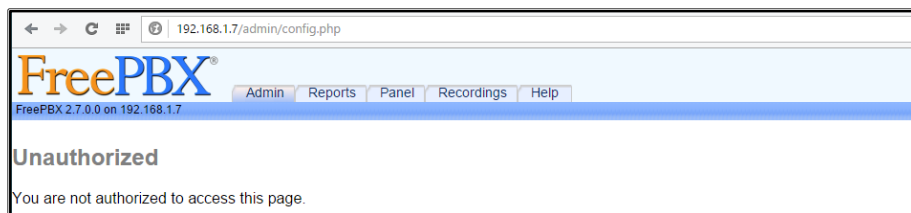


Figura 4.7 Módulo de FreePBX en la central telefónica “192.168.1.7”

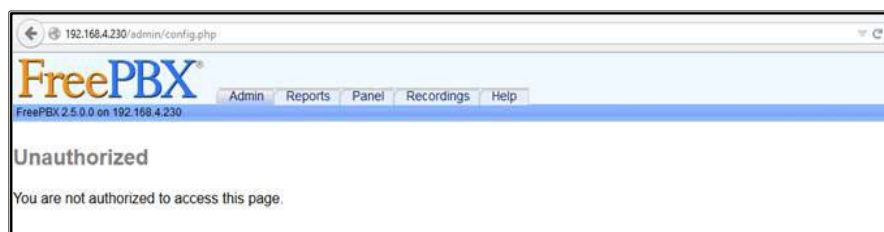


Figura 4.8 Módulo de FreePBX en la central telefónica “192.1684.230”

4.2.3 Reconocimiento de extensiones

La última fase de reconocimiento que se aplicará previo a la realización del análisis de vulnerabilidades, está enfocada en reconocer las extensiones que se encuentran creadas en las centrales telefónicas. El conocer los números de las extensiones telefónicas nos permitirá posteriormente desplegar ataques a las centrales telefónicas utilizando esta información.

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.

Comando:

```
root@kali:~# svwar 192.168.1.7 -e100-999 -m INVITE
```

Resultado:

Extension	Authentication
605	weird
768	weird
600	weird
210	weird
667	weird

Figura 4.9 Reconocimiento de extensiones en la central telefónica “192.168.1.7”

Comando:

```
root@kali:~# swwar 192.168.4.230 -e100-999 -m INVITE
```

Resultado:

Extension	Authentication
987	reqauth
801	reqauth
763	reqauth
769	reqauth
212	reqauth

Figura 4.10 Reconocimiento de extensiones en la central telefónica "192.168.4.230"

4.4 Ataques de interceptación

El protocolo de señalización **SIP** en la transmisión de la información envía los paquetes en texto plano, además, dentro de sus especificaciones técnicas no cuenta con una funcionalidad para cifrar la información que transmite.

En esta fase se realizará un ataque de interceptación, 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.

```
root@kali:~# ettercap -T -M ARP -i eth0 // //
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team
Listening on:
eth0 -> 00:0C:29:EF:06:8D
        192.168.4.128/255.255.255.0
        fe80::20c:29ff:feef:68d/64
```

Figura 4.11 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.

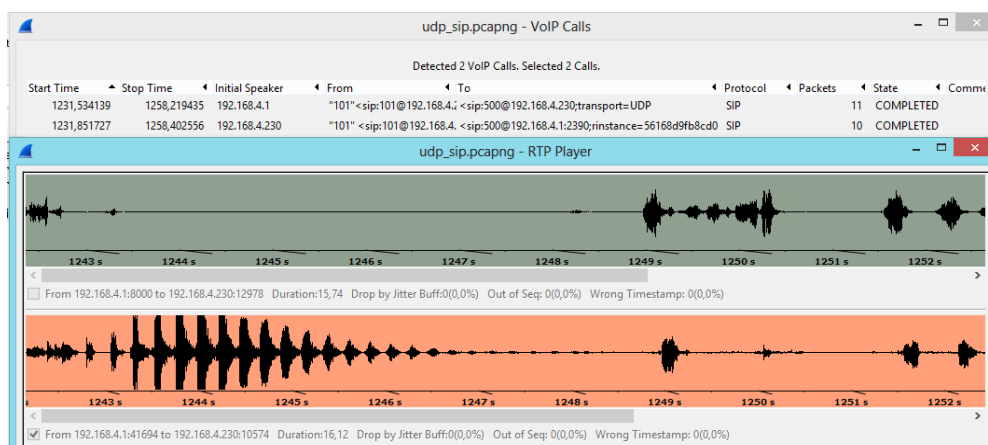


Figura 4.12 Captura de paquetes en las comunicaciones de VoIP y reproducción de audio de las conversaciones del personal de la organización

4.5 Ataques de denegación de servicios

En esta etapa se realizará un ataque de denegación de servicios, este vector de ataque tiene como finalidad causar la indisponibilidad o inoperancia de un servicio informático, además, origina que el servicio informático sea inutilizable para los usuarios. El servicio que se buscará causar su inoperancia, es la comunicación telefónica que utilizan los usuarios administrativos y los operadores del call center.

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.

Entre los parámetros necesarios para la ejecución de la herramienta “invitefood”, se utilizó una extensión **SIP** válida de la central telefónica víctima, previamente obtenida por los ataques de reconocimiento efectuados en el desarrollo de este capítulo, la cantidad de requerimientos que enviará la aplicación durante su ejecución es de diez millones de peticiones.

```
root@kali:~# inviteflood eth0 100 192.168.1.7 192.168.1.7 10000000
inviteflood - Version 2.0
                June 09, 2006
source IPv4 addr:port = 192.168.184.13:9
dest   IPv4 addr:port = 192.168.1.7:5060
targeted UA           = 100@192.168.1.7

Flooding destination with 10000000 packets
sent: 48749364
```

Figura 4.13 Ataque de denegación de servicio a la central telefónica “192.168.1.7”

```
root@kali:~# inviteflood eth0 500 192.168.4.230 192.168.4.230 10000000
inviteflood - Version 2.0
                June 09, 2006
source IPv4 addr:port = 192.168.184.13:9
dest   IPv4 addr:port = 192.168.4.230:5060
targeted UA           = 500@192.168.4.230

Flooding destination with 10000000 packets
sent: 393675200
```

Figura 4.14 Ataque de denegación de servicio a la central telefónica “192.168.4.230”

Durante la ejecución del ataque de denegación de servicios, el personal de sistemas de la organización realizó un monitoreo de las centrales telefónicas y observó algunas novedades causadas por el ataque de denegación de servicios, las cuales se expondrán a continuación:

Primero, 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.

```
-- Executing [500@from-sip-external:1] NoOp("SIP/9-b5269248", "Received incoming SIP connection from unknown peer to 500") in new stack
-- Executing [300@from-sip-external:2] Set("SIP/9-b5269248", "DID=500") in new stack
-- Executing [500@from-sip-external:3] Goto("SIP/9-b5269248", "s,1") in new stack
-- Goto (from-sip-external,s,1)
-- Executing [s@from-sip-external:1] GotoIf("SIP/9-b5269248", "0?from-trunk,500,1") in new stack
-- Executing [s@from-sip-external:2] Set("SIP/9-b5269248", "TIMEOUT(absolute)=15") in new stack
Channel will hangup at 2015-04-12 17:59:50.000 ECT.
-- Executing [s@from-sip-external:3] Answer("SIP/9-b5269248", "") in new stack
== Using SIP RTP TOS bits 184
== Using SIP RTP CoS mark 5
-- Executing [500@from-sip-external:1] NoOp("SIP/9-b52bee70", "Received incoming SIP connection from unknown peer to 500") in new stack
== Using SIP RTP TOS bits 184
== Using SIP RTP CoS mark 5
-- Executing [500@from-sip-external:1] NoOp("SIP/9-b525edf8", "Received incoming SIP connection from unknown peer to 500") in new stack
-- Executing [300@from-sip-external:2] Set("SIP/9-b525edf8", "DID=500") in new stack
```

Figura 4.15 CLI de la central telefónica “192.168.1.7” mostrando el ataque de denegación de servicios

```

-- Executing [100@from-sip-external:1] NoOp("SIP/192.168.20.199:9-0006dccc", "Received incoming SIP connection from unknown peer to 100") in new stack
-- Executing [100@from-sip-external:2] Set("SIP/192.168.20.199:9-0006dccc", "DID=100") in new stack
-- Executing [100@from-sip-external:3] Goto("SIP/192.168.20.199:9-0006dccc", "s,1") in new stack
-- Goto (from-sip-external,s,1)
-- Executing [s@from-sip-external:1] GotoIf("SIP/192.168.20.199:9-0006dccc", "0?checklang:noanonymous") in new stack
-- Goto (from-sip-external,s,5)
-- Executing [s@from-sip-external:5] Set("SIP/192.168.20.199:9-0006dccc", "TIMEOUT(absolute)=15") in new stack
Channel will hangup at 2015-04-12 18:12:49.577 ECT.
-- Executing [s@from-sip-external:6] Answer("SIP/192.168.20.199:9-0006dccc", "") in new stack
-- Executing [100@from-sip-external:1] NoOp("SIP/192.168.20.199:9-0006dccc", "Received incoming SIP connection from unknown peer to 100") in new stack
-- Executing [100@from-sip-external:2] Set("SIP/192.168.20.199:9-0006dccc", "DID=100") in new stack
-- Executing [100@from-sip-external:3] Goto("SIP/192.168.20.199:9-0006dccc", "s,1") in new stack
-- Goto (from-sip-external,s,1)
-- Executing [s@from-sip-external:1] GotoIf("SIP/192.168.20.199:9-0006dccc", "0?checklang:noanonymous") in new stack
-- Goto (from-sip-external,s,5)
-- Executing [s@from-sip-external:5] Set("SIP/192.168.20.199:9-0006dccc", "TIMEOUT(absolute)=15") in new stack
Channel will hangup at 2015-04-12 18:12:49.577 ECT.
-- Executing [s@from-sip-external:6] Answer("SIP/192.168.20.199:9-0006dccc", "") in new stack
-- Executing [100@from-sip-external:1] NoOp("SIP/192.168.20.199:9-0006dccc", "Received incoming SIP connection from unknown peer to 100") in new stack
-- Executing [100@from-sip-external:2] Set("SIP/192.168.20.199:9-0006dccc", "DID=100") in new stack

```

Figura 4.16 CLI de la central telefónica “192.168.4.230” mostrando el ataque de denegación de servicios

Segundo, 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.

```

top - 18:15:48 up 30 days, 11:44, 3 users, load average: 630.79, 827.66, 325.35
Tasks: 166 total, 1 running, 165 sleeping, 0 stopped, 0 zombie
Cpu(s): 6.4%us, 53.6%sy, 0.0%ni, 36.2%id, 0.0%wa, 0.0%hi, 3.7%si, 0.0%st
Mem: 3113984k total, 3004180k used, 109804k free, 144820k buffers
Swap: 5177336k total, 116k used, 5177220k free, 1960652k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 4093 root        16   0  820m 441m 7664  D 505.7 14.5 592:28.44 asterisk
 1 root        15   0  2152 688 572  S  0.0  0.0  0:00:00 init

```

Figura 4.17 Carga promedio de la central telefónica “192.168.1.7”, durante el ataque de denegación de servicios

```

1 [#####] 63.8% Tasks: 287 total, 17 running
2 [#####] 66.7% Load average: 2.08 0.72 0.26
3 [#####] 46.4% Uptime: 41 days, 16:01:11
4 [#####] 46.4%
Mem[|||||#####]565/3043MB
Swp[|] 0/2588MB

  PID USER      PRI  NI  VIRT  RES  SHR  S  CPU%  MEM%    TIME+  Command
  1 root        15   0  1944  644  552  S  0.0  0.0  0:04.56 init [2]
1466 root        21  -4  2176  604  340  S  0.0  0.0  0:00.14 ~- udevd --daemon
2277 daeron      16   0  1684  364  272  S  0.0  0.0  0:00.00 ~- /sbin/portmap
2508 root        16   0  1628  620  512  S  0.0  0.0  0:21.02 ~- /sbin/syslogd
2514 root        15   0  1576  380  308  S  0.0  0.0  0:00.04 ~- /sbin/klogd -x
2747 root        16   0  148M 88708 6852  S  0.7  3.8  0:00.09 ~- asterisk
2806 root        21   0  2672  1328 1072  S  0.0  0.1  0:00.00 ~- /bin/sh /usr/b

```

Figura 4.18 Carga promedio de la central telefónica “192.168.4.230”, 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, las personas que intentaban conectarse a la central telefónica no podían realizarlo exitosamente, por consiguiente, el servicio de “Asterisk” finalmente fue interrumpido y detenido por el sistema operativo al ser detectado como un proceso zombie en los servidores de las centrales telefónicas.

En la imagen siguiente se muestra el teléfono basado en software de los operadores del call center con los problemas presentados al no poderse autenticar en la central telefónica para poder realizar su gestión.



Figura 4.19 Estado de los teléfonos durante el ataque de denegación de servicios

4.6 Ataques por Fuerza Bruta

En esta fase, el vector de ataque que se desplegará está basado en la técnica de la fuerza bruta. Este tipo de ataque tiene como finalidad utilizar combinaciones de posibles claves para lograr tener acceso a un sistema informático con la clave correcta. Como objetivo de este análisis de vulnerabilidades, se buscará lograr una autenticación **SIP** en las centrales telefónicas, no obstante, ya contamos con un dato

previamente obtenido en la fase reconocimiento, el número de la extensión. Lo que resta es conocer la clave y para ello se utilizarán diccionarios de claves que serán procesados en conjunto con las extensiones con la finalidad de lograr la autenticación **SIP** a la central telefónica.

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.

```
root@kali:/diccionarios# crunch 3 10 "0123456789" > diccionario.txt
Crunch will now generate the following amount of data: 120987654000 bytes
115382 MB
112 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 11111111000
```

Figura 4.20 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 4.21 Ataque de fuerza bruta basada en diccionario a la extensión "101" de la central "192.168.4.230"

```
root@kali:~# svcrack -u 500 -d /diccionarios/diccionario.txt 192.168.4.230
ERROR:ASip0fRedWine:We got an unknown response
| Extension | Password |
-----
| 500       | 500      |
```

Figura 4.22 Ataque de fuerza bruta basada en diccionario a la extensión "500" de la central "192.168.4.230"

Como podemos observar en las imágenes precedentes, en la ejecución del comando se ha encontrado las claves de las extensiones utilizadas en el ataque de fuerza bruta basada en diccionario, las claves están compuestas por el mismo número de la extensión, ante esto, se evidencia una debilidad en la seguridad informática por la configuración de las extensiones **SIP** en las centrales telefónicas.

4.7 Explotación de Vulnerabilidades

En esta sección se obtendrá provecho de los hallazgos encontrados en el análisis de vulnerabilidades, esto es, con la finalidad de simular lo que haría un atacante con estas debilidades detectadas.

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.

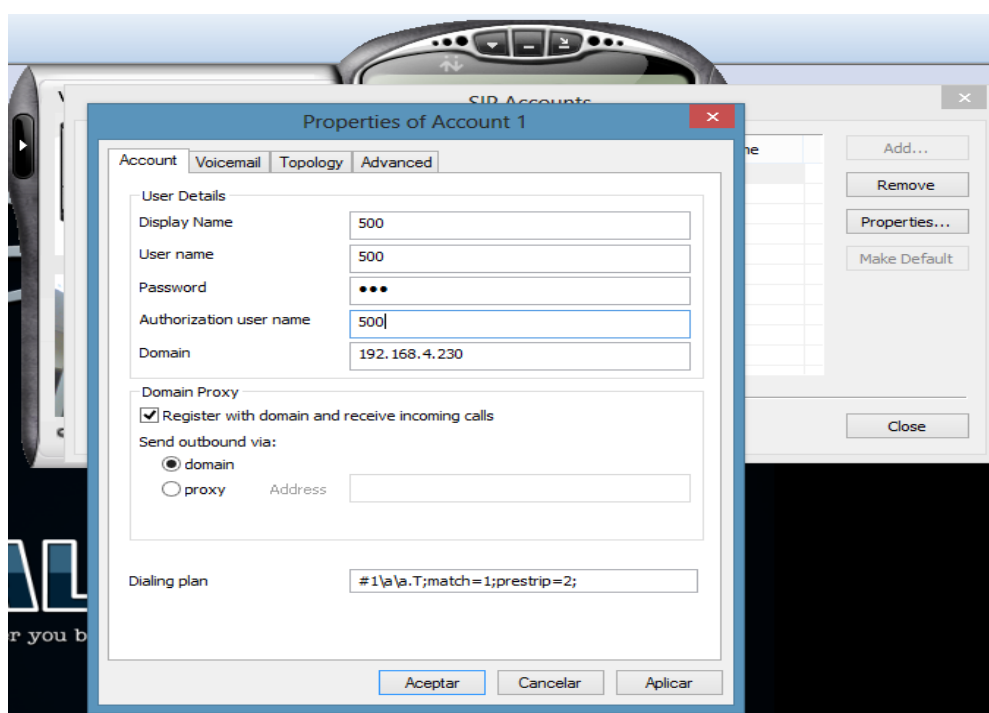


Figura 4.23 Autenticación a la central telefónica “192.168.4.230” desde la máquina atacante



Figura 4.24 Autenticación exitosa en la central “192.168.4.230” y generación de llamadas telefónicas desde la máquina atacante

Como podemos apreciar en la imagen precedente, una vez autenticado en la central telefónica se han generado llamadas a diferentes números destinos. En la estructura del **CDR** no se registra la dirección **IP** origen desde donde se realizan las llamadas, por lo tanto, en este registro no se identificará el origen de las llamadas que realicemos, es decir, el personal que revisa los **CDR** pensará que todas las llamadas realizadas son la extensión “500” que corresponden a un operador del call center.

CAPÍTULO 5

IMPLEMENTACIÓN DE SOLUCIONES DE SEGURIDAD INFORMÁTICA

5.1 Actualización del sistema

Inicialmente la medida de seguridad que se adoptará es la de realizar una actualización del software que utilizan las centrales telefónicas para las comunicaciones de **VoIP**. Las actualizaciones son necesarias en todo sistema informático para evitar vulnerabilidades inherentes al producto de software, los fabricantes de software generalmente están actualizando sus productos y liberando nuevas versiones con funcionalidades extras, correcciones de vulnerabilidades o errores detectados en versiones anteriores, generalmente, estas incidencias

son detectadas por el fabricante o por las comunidades de software que constantemente las reportan al fabricante.

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.

```
[root@tmkecpdc ~]# asterisk -r
Asterisk 13.3.2, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 13.3.2 currently running on tmkecpdc (pid = 1790)
tmkecpdc*CLI>
```

Figura 5.1 Versión actualizada de “Asterisk” en la central telefónica “192.168.4.230”

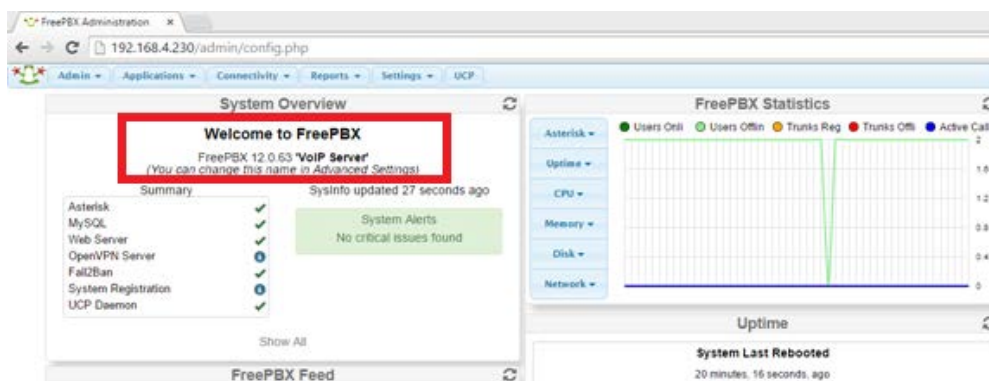


Figura 5.2 Versión actualizada de “FreePBX” en la central telefónica “192.168.4.230”

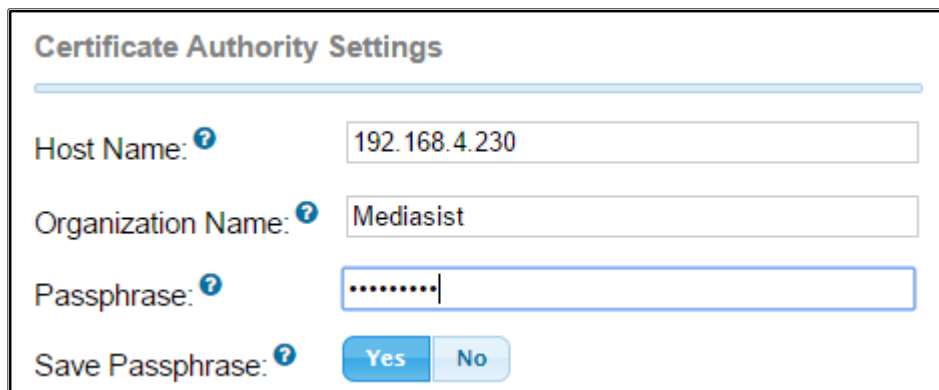
En la Figura 5.2 se puede apreciar al sistema “FreePBX” actualizado a su nueva versión, además, se muestra el tablero de comandos del sistema con una sección de alertas del sistema. En esta sección el sistema notificará las actualizaciones de seguridad disponibles para los módulos del sistema, por consiguiente, el administrador de las centrales telefónicas estará informado de las actualizaciones recientes para que puedan ser aplicadas inmediatamente en el sistema. En el tablero de comandos también se puede apreciar que la versión actualizada de “FreePBX” incluye un módulo de monitoreo para revisar el estado de utilización de los recursos de hardware tales como: procesador, memoria RAM, disco duro; además, se puede monitorear la cantidad de usuarios conectados a la central telefónica y el uso de las líneas telefónicas empleadas en las llamadas telefónicas del call center.

5.2 Cifrado en las comunicaciones de VoIP

El cifrado en las comunicaciones brindará un nivel de seguridad en la transmisión de la información que envían los protocolos de señalización utilizados en las comunicaciones de **VoIP** a través de la red de datos, por lo tanto, los atacantes que intercepten los paquetes en la red de datos no podrán descifrar fácilmente la información que se encuentra encriptada.

El cifrado de las comunicaciones se lo realizará con la utilización del protocolo criptográfico **TLS**, este protocolo utiliza certificados digitales para validar la autenticidad de los mensajes enviados por los involucrados en la comunicación, además, entre su funcionalidad existe un intercambio de llaves para cifrar y descifrar los mensajes, por consiguiente, la comunicación entre los involucrados será cifrada durante el intercambio de la información.

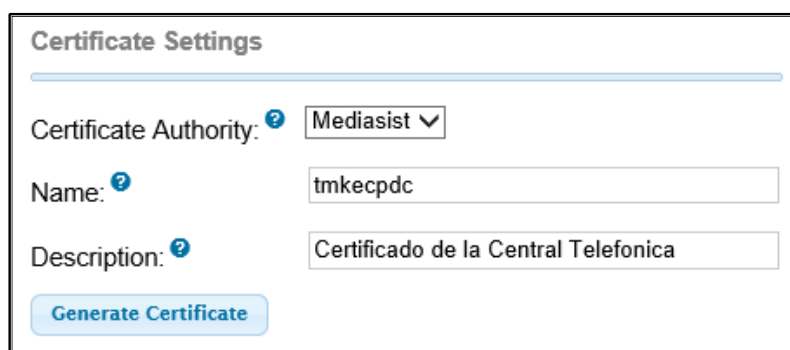
Inicialmente se procederá a crear la autoridad de certificación en la central telefónica, esta entidad será la encargada de la emisión y revocación de los certificados digitales. La aplicación "FreePBX" ya cuenta con un módulo para la creación de la autoridad certificadora y se lo utilizará especificando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



The screenshot shows a web form titled "Certificate Authority Settings". It contains four fields: "Host Name" with the value "192.168.4.230", "Organization Name" with the value "Mediasist", "Passphrase" with a masked input (dots), and "Save Passphrase" with radio buttons for "Yes" and "No".

Figura 5.3 Creación de la autoridad certificadora en la central telefónica "192.168.4.230"

Una vez creada la autoridad certificadora, lo siguiente que se realizará es la emisión de un certificado digital para el servidor de la central telefónica, esto es, debido a que en las comunicaciones de **VoIP** sobre **TLS** se necesita que la identidad digital de la central telefónica también pueda ser verificada.



The screenshot shows a web form titled "Certificate Settings". It contains three fields: "Certificate Authority" with a dropdown menu showing "Mediasist", "Name" with the value "tmkecpdc", and "Description" with the value "Certificado de la Central Telefonica". There is a "Generate Certificate" button at the bottom.

Figura 5.4 Emisión de certificado para la central telefónica "192.168.4.230"

También se emitirán certificados digitales para cada extensión telefónica, por consiguiente, el administrador de la central telefónica

podrá revocar los certificados individualmente de las extensiones telefónicas si la seguridad de alguno de ellos se encuentra comprometida.

The screenshot shows a 'Certificate Settings' window. It has three input fields: 'Certificate Authority' with a dropdown menu showing 'Mediasist', 'Name' with the text '500', and 'Description' with the text 'Certificado para el operador 500'. There is a blue button labeled 'Generate Certificate' at the bottom left of the window.

Figura 5.5 Emisión de certificado para la extensión "500" de la central telefónica "192.168.4.230"

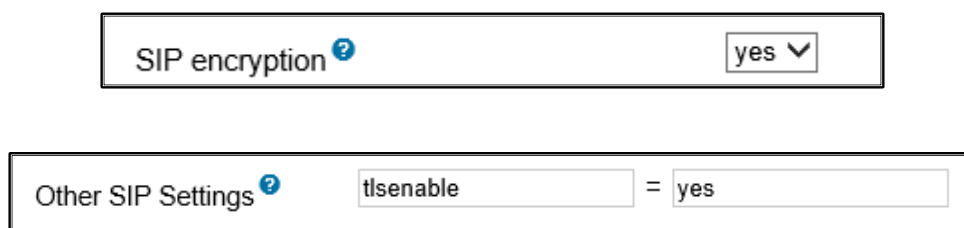
Los certificados digitales en el servidor de la central telefónica se almacenan en el directorio "/etc/asterisk/keys" como se muestra en la figura siguiente:

```
[root@tmkecpdc ~]# cd /etc/asterisk/keys/
[root@tmkecpdc keys]# ls
100.crt 103.crt 500.crt 503.crt 506.crt 509.crt 512.crt 515.crt 518.crt 521.crt 524.crt ca.cfg
100.csr 103.csr 500.csr 503.csr 506.csr 509.csr 512.csr 515.csr 518.csr 521.csr 524.csr ca.crt
100.key 103.key 500.key 503.key 506.key 509.key 512.key 515.key 518.key 521.key 524.key ca.key
100.pem 103.pem 500.pem 503.pem 506.pem 509.pem 512.pem 515.pem 518.pem 521.pem 524.pem ca.pem
101.crt 104.crt 501.crt 504.crt 507.crt 510.crt 513.crt 516.crt 519.crt 522.crt 525.crt default.crt
101.csr 104.csr 501.csr 504.csr 507.csr 510.csr 513.csr 516.csr 519.csr 522.csr 525.csr default.csr
101.key 104.key 501.key 504.key 507.key 510.key 513.key 516.key 519.key 522.key 525.key default.key
101.pem 104.pem 501.pem 504.pem 507.pem 510.pem 513.pem 516.pem 519.pem 522.pem 525.pem default.pem
102.crt 105.crt 502.crt 505.crt 508.crt 511.crt 514.crt 517.crt 520.crt 523.crt 700.crt tmkecpdc.crt
102.csr 105.csr 502.csr 505.csr 508.csr 511.csr 514.csr 517.csr 520.csr 523.csr 700.csr tmkecpdc.csr
102.key 105.key 502.key 505.key 508.key 511.key 514.key 517.key 520.key 523.key 700.key tmkecpdc.key
102.pem 105.pem 502.pem 505.pem 508.pem 511.pem 514.pem 517.pem 520.pem 523.pem 700.pem tmkecpdc.pem
```

Figura 5.6 Certificados digitales almacenados en 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.



The image shows two configuration fields. The first field is labeled "SIP encryption" with a help icon and a dropdown menu set to "yes". The second field is labeled "Other SIP Settings" with a help icon, containing a text input field for "tlsenable" followed by an equals sign and another text input field set to "yes".

Figura 5.7 Configuraciones avanzadas del protocolo SIP para la habilitación del cifrado en las comunicaciones de VoIP con el protocolo TLS

Port [?]	5060
Qualify [?]	yes
Qualify Frequency [?]	60
Transport [?]	All - TLS Primary ▼
Enable AVPF [?]	No ▼
Force AVP [?]	Yes ▼
Enable ICE Support [?]	Yes ▼
Enable Encryption [?]	Yes (SRTP only) ▼

Figura 5.8 Configuración del protocolo TLS y SRTP en la extensión telefónica "500" de la central telefónica "192.168.4.230"

Finalmente se asociarán las extensiones telefónicas con su respectivo certificado digital utilizando el protocolo **DTLS**, este protocolo permite tener privacidad en las conversaciones evitando accesos no permitidos o modificación en los mensajes durante la transmisión.

- DTLS	
Enable DTLS [?]	Yes ▼
Use Certificate [?]	500 ▼
DTLS Verify [?]	Certificate ▼
DTLS Setup [?]	Act/Pass ▼
DTLS Rekey Interval [?]	0

Figura 5.9 Configuración del protocolo DTLS para la extensión "500" de la central telefónica "192.168.4.230"

Las configuraciones del cifrado de las comunicaciones en una extensión **SIP** se aplican en el archivo de configuración “sip.conf” de la central telefónica como se muestra en la imagen siguiente.

```
[500]
deny=0.0.0.0/0.0.0.0
secret=f5d463f59045d96a88b8e32df8e61021
dtmfmode=rfc2833
canreinvite=no
context=from-internal
host=dynamic
trustpid=yes
sendrpid=pai
type=friend
nat=force_rport,comedia
port=5060
qualify=yes
qualifyfreq=60
transport=tls udp,tcp
avpr=no
force_avp=yes
icesupport=yes
encryption=yes
callgroup=
pickupgroup=
dial=SIP/500
permit=0.0.0.0/0.0.0.0
callerid=500 <500>
callcounter=yes
dtlshandle=yes
dtlsverify=certificate
dtlscertfile=/etc/asterisk/keys/500.pem
dtlscacfile=/etc/asterisk/keys/ca.crt
dtlssetup=actpass
dtlsrekey=0
```

Figura 5.10 Configuración del cifrado de las comunicaciones de VoIP en el archivo “sip.conf” de la extensión “500” en la central telefónica “192.168.4.230”

5.3 Listas de control de acceso

Las **ACL's** permitirán especificar las direcciones **IP** que estarán autorizadas para conectarse a determinadas extensiones de la central telefónica, es decir, solo podrán autenticarse los dispositivos cuya dirección **IP** esté especificada en la lista de los elementos permitidos, además, se puede especificar direcciones **IP** que formen parte de los elementos no permitidos.

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".

Deny ?	0.0.0.0/0.0.0.0
Permit ?	192.168.4.5/255.255.255.255

Figura 5.11 Configuración de la ACL en la extensión "500" de la central telefónica "192.168.4.230"

```
[500]
deny=0.0.0.0/0.0.0.0
secret=f5d463f59045d96a88b8e32df8e61021
dtmfmode=rfc2833
canreinvite=no
context=from-internal
host=dynamic
trustpid=yes
sendrpid=pai
type=friend
nat=force_rport,comedia
port=5060
qualify=yes
qualifyfreq=60
transport=tls,udp,tcp
avpf=no
force_avp=yes
icesupport=yes
encryption=yes
callgroup=
pickupgroup=
dial=STP/500
permit=192.168.4.5/255.255.255.255
callerid=500 <500>
callcounter=yes
faxdetect=no
cc_monitor_policy=generic
```

Figura 5.12 Configuración de la ACL en el archivo "sip.conf" para la extensión "500" de la central telefónica "192.168.4.230"

Como se puede apreciar en la Figura 5.12, la dirección **IP** "192.168.4.1" es la única que está permitida para conectarse a la central telefónica utilizando la extensión 500. En la sección "permit" se podrá agregar más de una dirección **IP** con permisos de conexión a la central telefónica utilizando esta extensión, cada extensión tiene su propia lista de control de acceso, además, se pueden especificar direcciones **IP** que no estarán permitidas utilizando la opción "deny".

5.4 Políticas de contraseñas

Tener una política de contraseñas en los procedimientos de sistemas es fundamental para proteger el acceso a los sistemas de la organización. Como se pudo evidenciar en los ataques de fuerza bruta realizados, las contraseñas estaban definidas por el número de la extensión y fueron encontradas fácilmente en un diccionario de claves numéricas.

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.

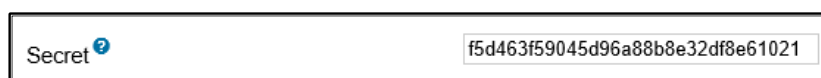


Figura 5.13 Contraseña generada por la aplicación “FreePBX” en la creación de una extensión

5.5 Seguridad perimetral

La implementación de un túnel **VPN** es necesaria en las comunicaciones telefónicas que se realizan a través del Internet, esto es, con la finalidad de cifrar los datos que se transmiten entre los dos

extremos que participan en la conexión, por consiguiente, la comunicación no podrá ser descifrada fácilmente por los atacantes.

Esta medida de seguridad se aplicará a las comunicaciones de **VoIP** que se realizan entre las distintas filiales de la organización mediante el uso del Internet. La conexión será cifrada mediante la utilización del protocolo **IPsec**, el cual es un conjunto de protocolos que cifran los paquetes que se transmiten en una conexión de datos, de esta manera se asegurará la comunicación entre dos centrales telefónicas remotas.

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 5. 14 Configuración de los parámetros criptográficos de la VPN IPsec

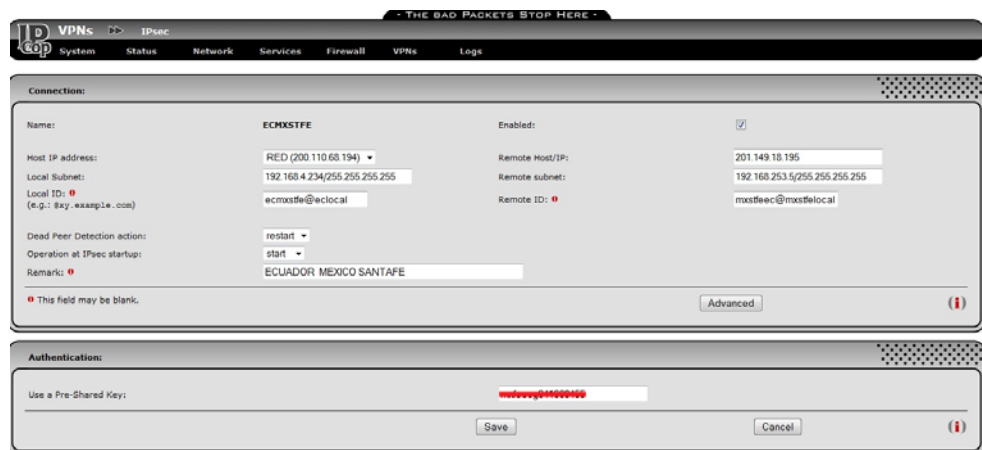


Figura 5.15 Conexión VPN entre las filiales de Guayaquil y México

5.6 Implementación del IPS

La implementación de un **IPS** es necesaria para la prevención de ataques por fuerza bruta y denegación de servicios, esto es, debido a las funcionalidades que tiene un sistema de prevención de intrusos para la detección de estos ataques e inmediatamente aplicar medidas basadas en políticas de seguridad.

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 5.16 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.


```

failregex = NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Wrong password
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Username/auth name mismatch
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - No matching peer found
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Not a local domain
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Peer is not supposed to register
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Device does not match ACL
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Device not configured to use this transport type
NOTICE.* *: No registration for peer '.*' \ (from <HOST>\)
NOTICE.* *: Host <HOST> failed MD5 authentication for '.*' \ (.*)

#
WARNING.* Ext. s: Friendly Scanner from <HOST>
WARNING.* *: .*Rejecting unknown SIP connection from <HOST>.*

```

Figura 5.17 Perfil de filtrado del Fail2ban para análisis de logs de la aplicación “Asterisk”

```

failregex = NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Wrong password
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Username/auth name mismatch
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - No matching peer found
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Not a local domain
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Peer is not supposed to register
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Device does not match ACL
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Device not configured to use this transport type
NOTICE.* *: No registration for peer '.*' \ (from <HOST>\)
NOTICE.* *: Host <HOST> failed MD5 authentication for '.*' \ (.*)
NOTICE.* *: Call from '.?' \ (<HOST>:.*\ ) to extension '.*' rejected

#
WARNING.* Ext. s: Friendly Scanner from <HOST>
WARNING.* *: .*Rejecting unknown SIP connection from <HOST>.*

```

Figura 5. 18 Perfil de filtrado del Fail2ban para análisis de logs de la aplicación “Asterisk”

Como se puede apreciar en la Figura 5.17 y 5.18, los perfiles de filtrado están basados en expresiones regulares para el análisis de los logs de la aplicación.

El Fail2ban utiliza “iptables” para realizar el bloqueo de las direcciones **IP** desde donde detecten los ataques de denegación de servicio y fuerza bruta, el iptables es una herramienta de cortafuegos que bloquea paquetes de datos dependiendo de las políticas de seguridad aplicadas.

CAPÍTULO 6

PRUEBAS DE LA SEGURIDAD INFORMÁTICA APLICADA

6.1 Validación del cifrado en las comunicaciones de VoIP

En esta sección se procederá a validar la efectividad de la medida de seguridad implementada con respecto al cifrado en las comunicaciones de **VoIP**. Para ello se instalarán teléfonos basados en software que soporten los protocolos de cifrado en las comunicaciones de **VoIP** tales como: **TLS** y **SRTP**. Los teléfonos basados en software que utiliza actualmente la organización no soportan los protocolos de cifrado en las comunicaciones, por lo tanto, para realizar las pruebas de seguridad se procederá a utilizar la aplicación “Zoiper” que tiene

soporte para los diversos protocolos necesarios en el cifrado de la información que se transmite a través de la conversación telefónica.

Inicialmente se realizará la configuración de la cuenta **SIP** con los datos de configuración de la cuenta como son: la dirección **IP** de la central telefónica, el usuario y la contraseña.

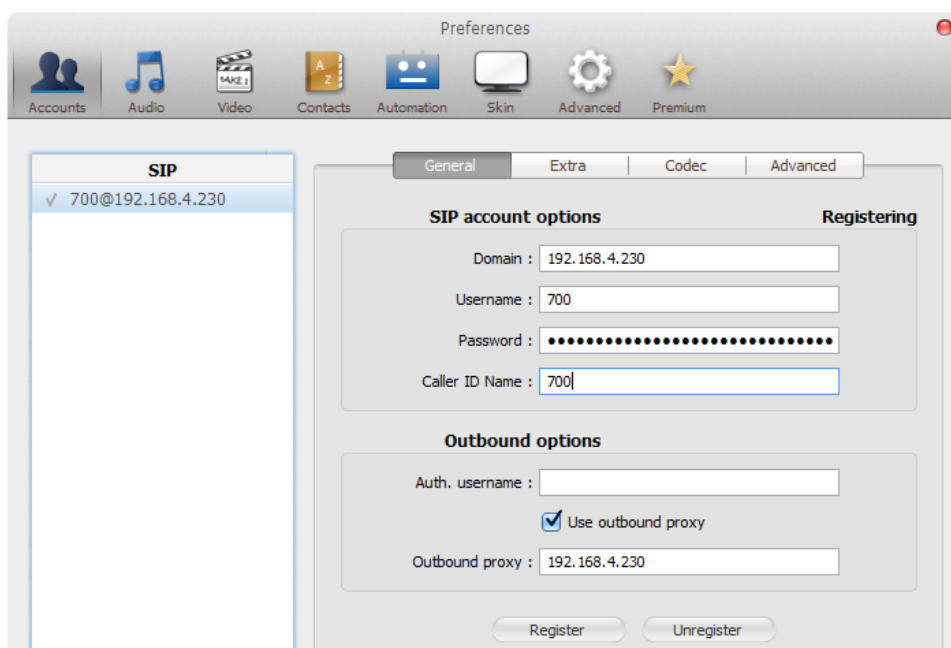


Figura 6.1 Configuración de la cuenta SIP en la aplicación "Zoiper"

Lo siguiente será especificar el directorio donde se encuentra el certificado digital que utilizará la extensión telefónica para que sea validada su identidad, además, el certificado será utilizado para el cifrado de la información en las conversaciones telefónicas mediante los protocolos de transmisión segura de la información. Los protocolos

a utilizar también son especificados en la configuración de la extensión telefónica, por lo tanto, se configurará los protocolos de comunicación segura como son **TLS** y **SRTP**.

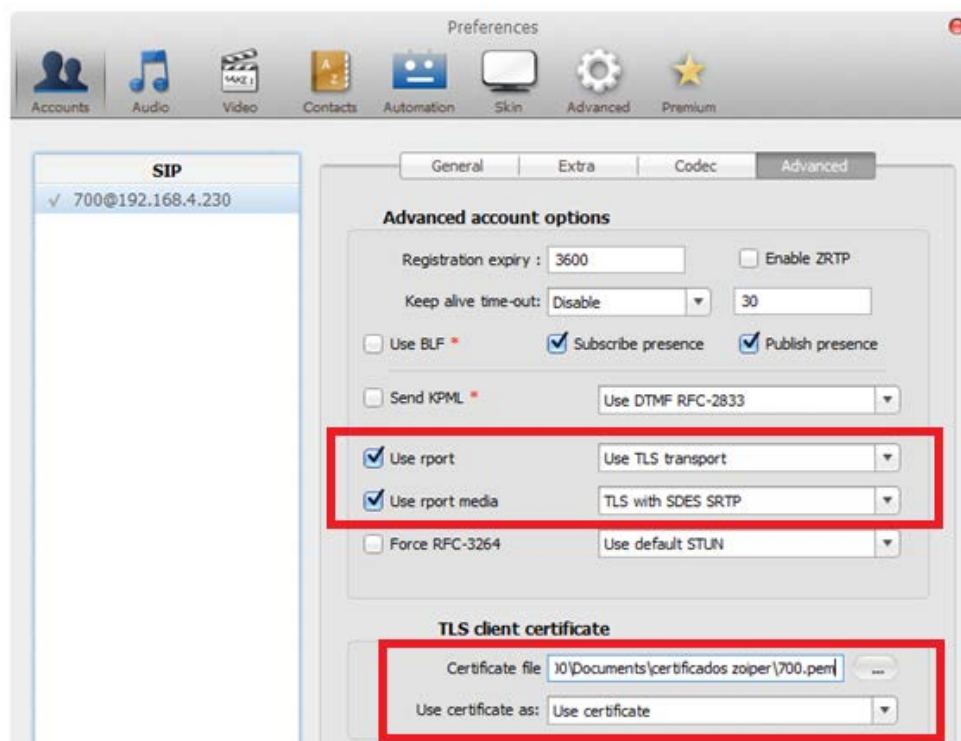


Figura 6.2 Configuración del certificado digital y protocolos de comunicaciones seguras en la aplicación "Zoiper"

Además se especificará el certificado digital de la autoridad de certificación en la aplicación "Zoiper", esto es, con la finalidad que no existen excepciones al momento de que el certificado digital de la extensión telefónica sea validada su confianza.

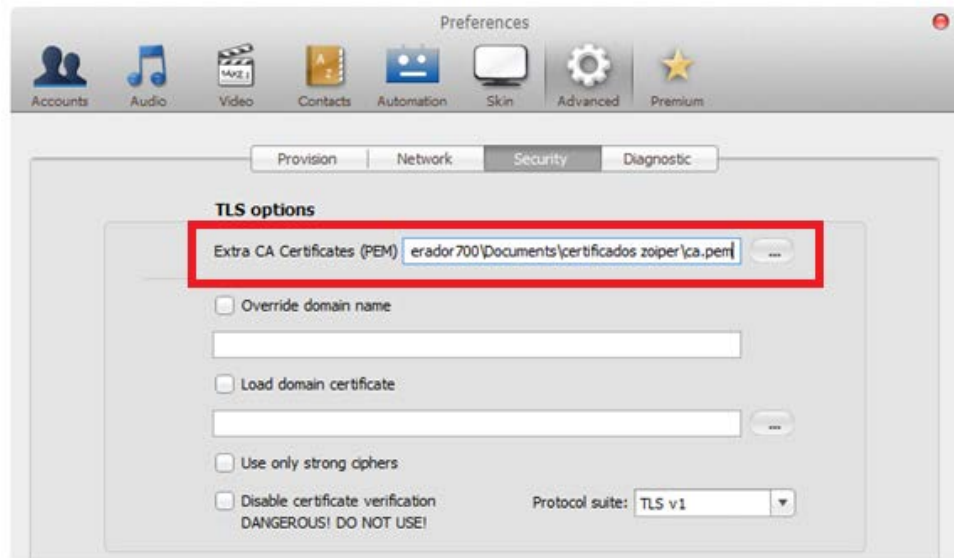


Figura 6.3 Configuración del certificado digital de la autoridad de certificación en la aplicación “Zoiper”

Una vez concluidas las configuraciones necesarias en la aplicación “Zoiper”, las extensiones están listas para empezar a ser utilizadas en las llamadas telefónicas.

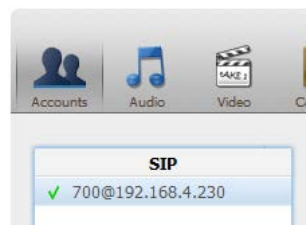


Figura 6.4 Autenticación exitosa a la central telefónica “192.168.4.230” de la extensión telefónica “700”

Finalmente, para validar la efectividad del mecanismo de seguridad, nuevamente se procedió a capturar los paquetes de datos en las

comunicaciones de **VoIP**. Los resultados que se encontraron en estas pruebas demuestran que las conversaciones telefónicas ya no pueden ser decodificadas y posteriormente reproducidas como se demuestra en la siguiente figura.

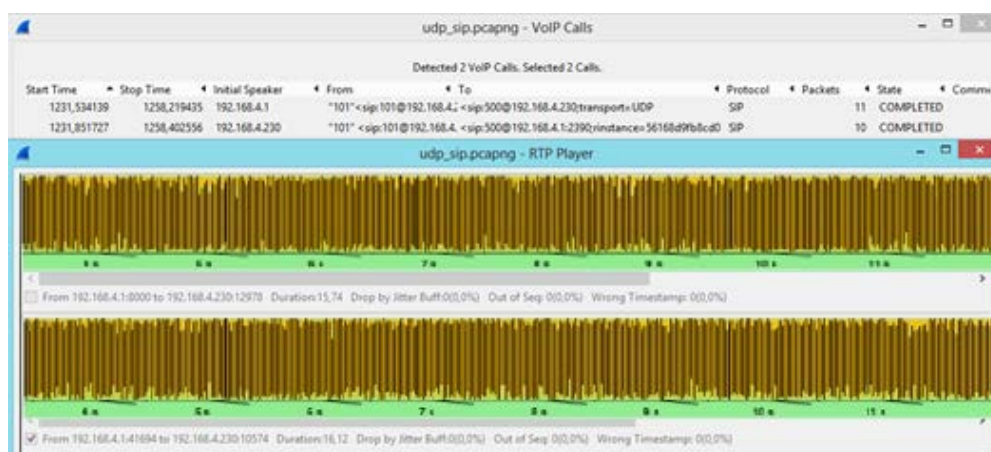


Figura 6.5 Validación del cifrado de las comunicaciones de VoIP por parte de los protocolos de comunicaciones seguras

6.2 Validación de la seguridad informática en las ACL's

En esta etapa de pruebas se validará la seguridad en las **ACL's** implementadas en las extensiones telefónicas, por lo tanto, se intentará realizar una autenticación **SIP** desde una dirección **IP** que no se encuentra autorizada en la lista de control de acceso.

Para llevar a cabo esta prueba, se intentará realizar una autenticación **SIP** con la extensión telefónica "500" desde la dirección **IP**: "192.168.4.1". En las listas de control de acceso solo está permitida la dirección **IP**: "192.168.4.5". Como podemos apreciar en la siguiente

imagen el resultado que se obtuvo fue un estado “403 forbidden”, que significa un estado de prohibido.



Figura 6.6 Estado de prohibido luego de tratar la autenticación SIP de la extensión “500”

En los registros de logs de la central telefónica se pudo validar la efectividad del funcionamiento de la **ACL**, esto es, debido a que se muestra que la dirección **IP**: “192.168.4.1” no está autorizada a realizar la autenticación de la extensión **SIP** “500”.

```
NOTICE[1892] chan_sip.c: Registration from '"500"<sip:500@192.168.4.230>' failed for '192.168.4.1:54772' - Device does not match ACL
NOTICE[1892] acl.c: SIP Peer ACL: Rejecting '192.168.4.1' due to a failure to pass ACL '(BASELINE)'
NOTICE[1892] chan_sip.c: Registration from '"500"<sip:500@192.168.4.230>' failed for '192.168.4.1:54772' - Device does not match ACL
```

Figura 6.7 Registros de logs de la central telefónica “192.168.4.230” mostrando la efectividad de la ACL

6.3 Validación de la seguridad informática en ataques de fuerza bruta

En esta sección se validará la efectividad de la seguridad contra los ataques de fuerza bruta, por consiguiente, se desplegará nuevamente un ataque de fuerza bruta sobre la central telefónica para validar la seguridad aplicada sobre este tipo de ataques.

Lo primero que se desplegará es el ataque de fuerza bruta basada en un diccionario de contraseñas, esto es, con la finalidad de verificar la funcionalidad del **IPS** quien debería actuar inmediatamente bloqueando este tipo de ataque sobre la central telefónica.

```
root@kali:/diccionarios# svcrack -u 500 -d /diccionarios/diccionario.txt 192.168.4.230
ERROR:ASipOfRedWine:no server response
WARNING:root:found nothing
```

Figura 6.8 Despliegue del ataque de fuerza bruta basado en un diccionario de claves aplicado a la extensión "500" de la central telefónica "192.168.4.230"

Inmediatamente luego de ejecutar el comando de ataque de fuerza bruta, se empezó a tener errores como "no server response" que significa que no existe respuesta por parte del servidor como se muestra en la Figura 6.8, además, luego se visualizaron errores en la ejecución como "stopping" que nos indica que durante la evaluación de cada clave del diccionario ha existido un error que no ha permitido conectarse a la central telefónica como se muestra en la Figura 6.9. Los errores presentados son el efecto de ya no contar con conexión a

la central telefónica, esto es, debido a la actuación inmediata del **IPS** bloqueando la dirección **IP** desde donde se ha realizado el ataque.

```
WARNING:ASipOfRedWine:It has been 1254.29595995 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 1254.30204701 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 1254.30794287 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 1254.31384587 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 1254.31998396 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 1254.32624507 seconds since we last received a response - stopping
```

Figura 6.9 Errores durante la ejecución del ataque de fuerza bruta a la central telefónica “192.168.4.230”

Para confirmar lo suscitado durante el ataque de fuerza bruta, se revisará los logs de la central telefónica y del **IPS** para verificar si efectivamente se bloqueó la dirección **IP** del atacante por la aplicación de los perfiles de filtrado del **IPS**. Como se puede apreciar en la Figura 6.10, los logs de la aplicación “Asterisk” evidencian los intentos de autenticación a la extensión **SIP** “500” de la central telefónica “192.168.4.230” por parte del atacante, además, en la Figura 6.11 se evidencia los logs de la aplicación “Fail2ban”, donde se muestra que la dirección **IP** del atacante “192.168.4.128” ha sido bloqueada por el **IPS** utilizando “iptables”.

```
NOTICE[1882] chan_sip.c: Registration from ""500" <sip:500@192.168.4.230>' failed for '192.168.4.128:5060' - Wrong password
NOTICE[1882] chan_sip.c: Registration from ""500" <sip:500@192.168.4.230>' failed for '192.168.4.128:5060' - Wrong password
NOTICE[1882] chan_sip.c: Registration from ""500" <sip:500@192.168.4.230>' failed for '192.168.4.128:5060' - Wrong password
NOTICE[1882] chan_sip.c: Registration from ""500" <sip:500@192.168.4.230>' failed for '192.168.4.128:5060' - Wrong password
NOTICE[1882] chan_sip.c: Registration from ""500" <sip:500@192.168.4.230>' failed for '192.168.4.128:5060' - Wrong password
```

Figura 6.10 Log de “Asterisk” evidenciando los intentos de autenticación a la extensión “500” de la central telefónica “192.168.4.230”

```

[root@tmkecpdc ~]# tail -f /var/log/fail2ban.log
2015-05-06 00:24:32,566 fail2ban.actions: INFO Set banTime = 1800
2015-05-06 00:24:32,616 fail2ban.jail : INFO Jail 'recidive' started
2015-05-06 00:24:32,715 fail2ban.jail : INFO Jail 'ssh-iptables' started
2015-05-06 00:24:32,859 fail2ban.jail : INFO Jail 'apache-badbots' started
2015-05-06 00:24:32,967 fail2ban.jail : INFO Jail 'pbx-gui' started
2015-05-06 00:24:33,131 fail2ban.jail : INFO Jail 'asterisk-iptables' started
2015-05-06 00:24:33,204 fail2ban.jail : INFO Jail 'apache-tcpwrapper' started
2015-05-06 00:26:07,384 fail2ban.actions: WARNING [asterisk-iptables] Ban 192.168.4.128
2015-05-06 00:26:07,608 fail2ban.actions: INFO [asterisk-iptables] 192.168.4.128 already banned

```

Figura 6.11 Log de “Fail2ban evidenciando el bloqueo aplicado a la dirección IP “192.168.4.128”

6.4 Validación de la seguridad informática en ataques de denegación de servicios

En esta etapa se procederá a validar la efectividad de la seguridad informática aplicada ante los ataques de denegación de servicios, esto es, realizando nuevamente el ataque de denegación de servicios mediante la inundación de requerimientos **SIP** de inicio de sesión “INVITE”.

Se desplegará nuevamente el ataque de denegación de servicios sobre la central telefónica “192.168.4.230” utilizando la extensión “500”, como podemos apreciar en la Figura 6.12 el ataque inicialmente no ha presentado ningún tipo de error durante su ejecución.

```

root@kali:~# inviteflood eth0 500 192.168.4.230 192.168.4.230 10000000
inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port = 192.168.4.128:9
dest   IPv4 addr:port = 192.168.4.230:5060
targeted UA           = 500@192.168.4.230

Flooding destination with 10000000 packets
sent: 3650564

```

Figura 6.12 Ejecución del ataque de denegación de servicios sobre la central telefónica “192.168.4.230” utilizando la extensión “500”

Sin embargo, en el monitoreo realizado a la central telefónica podemos apreciar que la **IP** del atacante ha sido bloqueada por el **IPS** demostrando la efectividad de la seguridad informática aplicada, esto es, debido a que este tipo de ataques se encuentran en los perfiles de filtrado del **IPS** y el bloqueo se ha sido realizado por las políticas establecidas en la aplicación “Fail2ban”.

```

[root@tmkecpdc ~]# tail -f /var/log/fail2ban.log
2015-05-13 02:45:57,777 fail2ban.filter : INFO Set findtime = 600
2015-05-13 02:45:57,778 fail2ban.actions: INFO Set banTime = 1800
2015-05-13 02:45:57,805 fail2ban.jail : INFO Jail 'recidive' started
2015-05-13 02:45:57,836 fail2ban.jail : INFO Jail 'ssh-iptables' started
2015-05-13 02:45:57,887 fail2ban.jail : INFO Jail 'apache-badbots' started
2015-05-13 02:45:57,927 fail2ban.jail : INFO Jail 'pbx-gui' started
2015-05-13 02:45:57,972 fail2ban.jail : INFO Jail 'asterisk-iptables' started
2015-05-13 02:45:58,021 fail2ban.jail : INFO Jail 'apache-tcpwrapper' started
2015-05-13 02:45:58,061 fail2ban.jail : INFO Jail 'xftpd-iptables' started
2015-05-13 02:46:00,112 fail2ban.actions: WARNING [asterisk-iptables] Ban 192.168.4.128

```

Figura 6.13 Log de “Fail2ban evidenciando el bloqueo aplicado a la dirección IP “192.168.4.128”

6.5 Análisis de 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 interceptación, 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 Y RECOMENDACIONES

Conclusiones:

1. 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.
2. 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.

3. 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:

1. Mantener revisiones periódicas de las nuevas actualizaciones de seguridad sobre los componentes que pueden ser aplicados a la infraestructura de comunicaciones telefónicas.
2. Establecer una planificación de auditorías sobre la seguridad informática de la infraestructura de comunicaciones **VoIP**.
3. 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.
4. 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.
5. Implementar un sistema de gestión de la seguridad de la información basada en estándares internacionales como por ejemplo la norma: ISO 27001-2008.

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.

ANEXOS

ANEXO A. Resultados del escaneo de puertos con la herramienta NMAP

Starting Nmap 6.47 (<http://nmap.org>) at 2015-05-10 16:24 ECT

NSE: Loaded 118 scripts for scanning.

NSE: Script Pre-scanning.

Initiating Ping Scan at 16:24

Scanning 192.168.4.230 [4 ports]

Completed Ping Scan at 16:24, 0.10s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 16:24

Completed Parallel DNS resolution of 1 host. at 16:24, 0.00s elapsed

Initiating SYN Stealth Scan at 16:24

Scanning 192.168.4.230 [1000 ports]

Discovered open port 113/tcp on 192.168.4.230

Discovered open port 139/tcp on 192.168.4.230

Discovered open port 111/tcp on 192.168.4.230

Discovered open port 22/tcp on 192.168.4.230

Discovered open port 80/tcp on 192.168.4.230

Discovered open port 445/tcp on 192.168.4.230

Discovered open port 3306/tcp on 192.168.4.230

Discovered open port 1720/tcp on 192.168.4.230

Discovered open port 2000/tcp on 192.168.4.230

Discovered open port 8086/tcp on 192.168.4.230

adjust_timeouts2: packet supposedly had rtt of 13098827 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 13098827 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 13142469 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 13142469 microseconds. Ignoring time.

Increasing send delay for 192.168.4.230 from 0 to 5 due to 382 out of 954 dropped probes since last increase.

Completed SYN Stealth Scan at 16:25, 45.78s elapsed (1000 total ports)

Initiating Service scan at 16:25

Scanning 10 services on 192.168.4.230

Completed Service scan at 16:27, 131.35s elapsed (10 services on 1 host)

Initiating OS detection (try #1) against 192.168.4.230

Retrying OS detection (try #2) against 192.168.4.230

Initiating Traceroute at 16:27

Completed Traceroute at 16:27, 0.03s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 16:27

Completed Parallel DNS resolution of 2 hosts. at 16:27, 0.42s elapsed

NSE: Script scanning 192.168.4.230.

Initiating NSE at 16:27

Completed NSE at 16:27, 21.33s elapsed

Nmap scan report for 192.168.4.230

Host is up (0.040s latency).

Not shown: 989 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 4.3p2 Debian 9etch3 (protocol 2.0)
--------	------	-----	--

| ssh-hostkey:

| 1024 0e:55:ba:5f:03:63:eb:aa:ba:0f:e7:d2:53:34:b1:57 (DSA)

|_ 2048 9b:55:d0:fe:73:03:d0:de:52:82:02:a6:10:5c:9a:e3 (RSA)

80/tcp open http Apache httpd 2.2.3 ((Debian) PHP/5.2.0-8+etch13)

| http-methods: GET HEAD POST OPTIONS TRACE

| Potentially risky methods: TRACE

|_ See <http://nmap.org/nsedoc/scripts/http-methods.html>

|_ http-title: FreePBX

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 32768/udp status

|_ 100024 1 45938/tcp status

113/tcp open ident

139/tcp open netbios-ssn Samba smbd 3.X (workgroup: GEAECPCD)

445/tcp open netbios-ssn Samba smbd 3.X (workgroup: GEAECPCD)

514/tcp filtered shell

1720/tcp open H.323/Q.931?

2000/tcp open cisco-sccp?

3306/tcp open mysql MySQL 5.0.32-Debian_7etch6-log

| mysql-info:

| Protocol: 53

| Version: .0.32-Debian_7etch6-log

| Thread ID: 26867481

| Capabilities flags: 41516

| Some Capabilities: SupportsTransactions, SupportsCompression, Support41Auth, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag

| Status: Autocommit

|_ Salt: #]0swyxqMIZ\@giZhylA

8086/tcp open d-s-n?

Device type: general purpose|storage-misc|VoIP phone

Running (JUST GUESSING): Linux 2.4.X|3.X (98%), Microsoft Windows 7|XP (95%), BlueArc embedded (91%), Pirelli embedded (88%)

OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:3
cpe:/o:microsoft:windows_7::enterprise cpe:/o:microsoft:windows_xp::sp3
cpe:/h:bluearc:titan_2100 cpe:/h:pirelli:dp-10

Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (98%), Linux 3.2 (96%), Microsoft Windows 7 Enterprise (95%), Microsoft Windows XP SP3 (95%), BlueArc Titan 2100 NAS device (91%), Pirelli DP-10 VoIP phone (88%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=243 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

| nbstat: NetBIOS name: TMKECPDC, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| Names:

| TMKECPDC<00> Flags: <unique><active>

| TMKECPDC<03> Flags: <unique><active>

| TMKECPDC<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| GEAECPCD<1d> Flags: <unique><active>
| GEAECPCD<1e> Flags: <group><active>
|_ GEAECPCD<00> Flags: <group><active>
| smb-os-discovery:
| OS: Unix (Samba 3.0.24)
| NetBIOS computer name:
| Workgroup: GEAECPCD
|_ System time: 2015-05-10T16:27:40-05:00
| smb-security-mode:
| Account that was used for smb scripts: guest
| Share-level authentication (dangerous)
| SMB Security: Challenge/response passwords supported
|_ Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	0.13 ms	192.168.184.2
2	0.16 ms	192.168.4.230

NSE: Script Post-scanning.

Initiating NSE at 16:27

Completed NSE at 16:27, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 213.74 seconds

Raw packets sent: 1665 (76.536KB) | Rcvd: 1216 (49.300KB)

Starting Nmap 6.47 (<http://nmap.org>) at 2015-05-10 16:38 ECT

NSE: Loaded 118 scripts for scanning.

NSE: Script Pre-scanning.

Initiating Ping Scan at 16:38

Scanning 192.168.1.6 [4 ports]

Completed Ping Scan at 16:38, 0.11s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 16:38

Completed Parallel DNS resolution of 1 host. at 16:38, 0.14s elapsed

Initiating SYN Stealth Scan at 16:38

Scanning 192.168.1.6 [1000 ports]

Discovered open port 22/tcp on 192.168.1.6

Discovered open port 111/tcp on 192.168.1.6

Discovered open port 3306/tcp on 192.168.1.6

Discovered open port 80/tcp on 192.168.1.6

Discovered open port 53/tcp on 192.168.1.6

Increasing send delay for 192.168.1.6 from 0 to 5 due to 203 out of 507 dropped probes since last increase.

adjust_timeouts2: packet supposedly had rtt of 14119450 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 14119450 microseconds. Ignoring time.

Discovered open port 4445/tcp on 192.168.1.6

Completed SYN Stealth Scan at 16:39, 59.12s elapsed (1000 total ports)

Initiating Service scan at 16:39

Scanning 6 services on 192.168.1.6

Completed Service scan at 16:41, 131.60s elapsed (6 services on 1 host)

Initiating OS detection (try #1) against 192.168.1.6

Retrying OS detection (try #2) against 192.168.1.6

Initiating Traceroute at 16:42

Completed Traceroute at 16:42, 0.02s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 16:42

Completed Parallel DNS resolution of 2 hosts. at 16:42, 0.22s elapsed

NSE: Script scanning 192.168.1.6.

Initiating NSE at 16:42

Completed NSE at 16:42, 30.09s elapsed

Nmap scan report for 192.168.1.6

Host is up (0.036s latency).

Not shown: 993 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
--------	------	-----	----------------------------

| ssh-hostkey:

| 1024 95:e2:bd:82:c8:68:69:e9:91:37:7b:02:5f:10:c8:ee (DSA)

|_ 2048 f5:84:07:b8:e4:55:b1:a5:c0:9f:fb:64:67:54:4a:70 (RSA)

53/tcp	open	domain	dnsmasq 2.45
--------	------	--------	--------------

| dns-nsid:

|_ bind.version: dnsmasq-2.45

80/tcp	open	http	Apache httpd 2.2.3 ((CentOS))
--------	------	------	-------------------------------

| http-methods: GET HEAD POST OPTIONS TRACE

| Potentially risky methods: TRACE

|_ See <http://nmap.org/nsedoc/scripts/http-methods.html>

| http-robots.txt: 1 disallowed entry

|_

|_http-title: FreePBX

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 677/udp status

|_ 100024 1 680/tcp status

514/tcp filtered shell

3306/tcp open mysql MySQL (unauthorized)

4445/tcp open upnotifyp?

Device type: general purpose|storage-misc

Running (JUST GUESSING): Linux 2.4.X|3.X (98%), Microsoft Windows 7|XP (96%), BlueArc embedded (91%)

OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:3

cpe:/o:microsoft:windows_7:::enterprise cpe:/o:microsoft:windows_xp:::sp3

cpe:/h:bluearc:titan_2100

Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (98%), Linux 3.2 (98%), Microsoft Windows 7 Enterprise (96%), Microsoft Windows XP SP3 (96%), BlueArc Titan 2100 NAS device (91%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=260 (Good luck!)

IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.28 ms 192.168.184.2

2 0.36 ms 192.168.1.6

NSE: Script Post-scanning.

Initiating NSE at 16:42

Completed NSE at 16:42, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 235.72 seconds

Raw packets sent: 1807 (82.780KB) | Rcvd: 1081 (43.848KB)

Starting Nmap 6.47 (<http://nmap.org>) at 2015-05-10 16:46 ECT

NSE: Loaded 118 scripts for scanning.

NSE: Script Pre-scanning.

Initiating Ping Scan at 16:46

Scanning 192.168.1.7 [4 ports]

Completed Ping Scan at 16:46, 0.07s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 16:46

Completed Parallel DNS resolution of 1 host. at 16:46, 0.45s elapsed

Initiating SYN Stealth Scan at 16:46

Scanning 192.168.1.7 [1000 ports]

Discovered open port 80/tcp on 192.168.1.7

Discovered open port 111/tcp on 192.168.1.7

Discovered open port 53/tcp on 192.168.1.7

Discovered open port 22/tcp on 192.168.1.7

Discovered open port 3306/tcp on 192.168.1.7

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

adjust_timeouts2: packet supposedly had rtt of 13179402 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 13179402 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 13286011 microseconds. Ignoring time.

adjust_timeouts2: packet supposedly had rtt of 13286011 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 13276324 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 13276324 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 13231565 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 13231565 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 13291515 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 13291515 microseconds. Ignoring time.
Increasing send delay for 192.168.1.7 from 0 to 5 due to 379 out of 946 dropped probes
since last increase.

Discovered open port 4445/tcp on 192.168.1.7

Completed SYN Stealth Scan at 16:47, 39.10s elapsed (1000 total ports)

Initiating Service scan at 16:47

Scanning 6 services on 192.168.1.7

Completed Service scan at 16:49, 131.58s elapsed (6 services on 1 host)

Initiating OS detection (try #1) against 192.168.1.7

Retrying OS detection (try #2) against 192.168.1.7

Initiating Traceroute at 16:49

Completed Traceroute at 16:49, 0.02s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 16:49

Completed Parallel DNS resolution of 2 hosts. at 16:49, 0.39s elapsed

NSE: Script scanning 192.168.1.7.

Initiating NSE at 16:49

Completed NSE at 16:50, 30.13s elapsed

Nmap scan report for 192.168.1.7

Host is up (0.036s latency).

Not shown: 993 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.3 (protocol 2.0)

| ssh-hostkey:

| 1024 c8:f2:3e:51:e8:eb:5d:c2:91:5e:70:7e:28:51:6d:6a (DSA)

|_ 2048 55:4e:27:1d:c6:27:bf:28:c1:bf:36:27:3a:c7:41:68 (RSA)

53/tcp open domain dnsmasq 2.45

| dns-nsid:

|_ bind.version: dnsmasq-2.45

80/tcp open http Apache httpd 2.2.3 ((CentOS))

| http-methods: GET HEAD POST OPTIONS TRACE

| Potentially risky methods: TRACE

|_ See <http://nmap.org/nsedoc/scripts/http-methods.html>

| http-robots.txt: 1 disallowed entry

|_ /

|_ http-title: FreePBX

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 639/udp status

|_ 100024 1 642/tcp status

514/tcp filtered shell

3306/tcp open mysql?

|_mysql-info: ERROR: Script execution failed (use -d to debug)

4445/tcp open upnotifyp?

Device type: general purpose|storage-misc|VoIP phone

Running (JUST GUESSING): Linux 2.4.X|3.X (98%), Microsoft Windows 7|XP (96%), BlueArc embedded (91%), Pirelli embedded (88%)

OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:3
cpe:/o:microsoft:windows_7::enterprise cpe:/o:microsoft:windows_xp::sp3
cpe:/h:bluearc:titan_2100 cpe:/h:pirelli:dp-10

Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (98%), Linux 3.2 (98%), Microsoft Windows 7 Enterprise (96%), Microsoft Windows XP SP3 (96%), BlueArc Titan 2100 NAS device (91%), Pirelli DP-10 VoIP phone (88%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=259 (Good luck!)

IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.21 ms 192.168.184.2

2 0.17 ms 192.168.1.7

NSE: Script Post-scanning.

Initiating NSE at 16:50

Completed NSE at 16:50, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at
<http://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 216.31 seconds

Raw packets sent: 1620 (74.552KB) | Rcvd: 1157 (46.888KB)