ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PARA CONFIGURAR CENTRALES VOIP"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

DIANA YOCONDA JARAMILLO RODAS

GUAYAQUIL-ECUADOR

AÑO: 2015

AGRADECIMIENTO

Principalmente a Dios por otorgarme la sabiduría y la salud para la finalización de este trabajo.

Gracias a mi familia y amigos por impulsarme a seguir adelante y su colaboración durante el desarrollo de este trabajo.

Gracias también a los profesores por las enseñanzas brindadas que ayudaron a formarme en esta etapa profesional.

DEDICATORIA

Dedico este trabajo con todo mi amor a mi familia por su apoyo incondicional para cumplir mis metas profesionales.

TRIBUNAL DE SUSTENTACIÓN

MGS LAURA URETA

PROFESOR DELEGADO POR LA MAESTRÍA DE INFORMACIÓN GERENCIAL

MGS LENIN FREIRE

PROFESOR DELEGADO POR LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

RESUMEN

El presente proyecto tiene como objetivo implementar un esquema de seguridad en un ambiente de laboratorio, que garantice la mayor mitigación a ataques informáticos, que podrían causar una intrusión no autorizada en la central VoIP.

En el capítulo 1 se abordará la problemática de la seguridad en la redes de VoIP, así como también sus posibles soluciones.

En el capítulo 2 se referirá a un análisis de los vectores de ataques tanto internos como externos, las herramientas utilizadas para descubrir posibles vulnerabilidades en una central Elastix 2.5 instalada por defecto, e igualmente abordará las implementaciones de controles de seguridad.

En el capítulo 3 se analizará los resultados obtenidos del impacto sobre la infraestructura VoIP de posibles vulnerabilidades y las soluciones propuestas

para mitigarlas, que afectan a los tres pilares más importantes de la seguridad: disponibilidad, integridad y confidencialidad.

Por último se emitirán las conclusiones y recomendaciones del presente trabajo

ÍNDICE GENERAL

ABREVIATURAS

DoS	Denial of Service
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
PSTN	public switched telephone network
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SSH	Secure SHell
TLS	Transport Layer Security
VoIP	Voice over IP

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La VoIP es una tecnología ampliamente utilizada que está en auge y como tal presenta varios desafíos, como la seguridad, debido a que está basada en el protocolo IP, el cual por sí solo es inseguro. Por tanto esta tecnología puede tener varios problemas de seguridad y ser vulnerable a ataques internos y/o externos a través de Internet.

Esta tesis a través del análisis de varios vectores de ataques pretende ser una guía para identificar las debilidades existentes en una infraestructura VoIP, con el fin de fortalecer la protección y de esta manera evitar ser susceptibles a ataques por personas no autorizadas.

Se trabajará en una ambiente de laboratorio con una central Elastix 2.5 instalada por defecto, la cual cuenta con cinco extensiones, dos de las cuales serán remotas. Se asumirá que el sistema VoIP debe tener funcionalidad 24/7, lo cual significa que tiene que ser suficientemente seguro para soportar posibles ataques.

Esta propuesta le será muy útil a un administrador de seguridad para examinar su infraestructura VoIP, ya que es importante realizar un análisis desde el punto de vista del atacante para descubrir las partes más vulnerables del sistema, tener el conocimiento de las herramientas que se podrían utilizar para atacar a la infraestructura VoIP es crucial.

El problema que esta tesis resuelve es relevante para cualquier empresa que utilice la tecnología de VoIP, ya que a menudo se da importancia a características tales como la calidad de servicio, pero las amenazas de seguridad no son analizadas y no son tomadas en consideración.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

La gran mayoría de empresas gracias a los avances de la tecnología están migrando de la telefonía tradicional (PSTN), a la revolucionaria telefonía IP (VoIP), algunas de las motivaciones son los bajos costos de la telefonía IP comparados con la telefonía tradicional, otra y tal vez la más diferenciadora de la telefonía tradicional, es que si se tiene la central IP conectada al internet, un usuario de la misma puede realizar una llamada desde cualquier parte del mundo que exista conectividad a internet, lo cual constituye una ventaja para las personas que viajan frecuentemente.

El problema principal cuando se implementan centrales VoIP es que se da prioridad al funcionamiento como tal de la central, es decir al envío/recepción de voz, datos, calidad de servicio etc, y no a la seguridad, es decir existe una falta de concienciación en el campo de seguridad, en algunos casos las empresas tienen la mentalidad que jamás serán atacadas. Las empresas aprenden de los errores como por ejemplo: pagar elevadas facturas, sufrir intrusiones en sus sistemas que causen un daño al negocio que realizan o uno de imagen. Una central de VoIP requiere una buena configuración que impida a un atacante explotar el sistema en beneficio propio, para lo cual se necesita altos conocimientos de seguridad.

La telefonía IP (VoIP) se basa en el protocolo IP, el cual de por sí es poco seguro, debido a que cuando se implementó no se pensó en la seguridad, la cual ha sido un camino al andar conforme ha avanzado el tiempo. Otros de los protocolos utilizados en VoIP son SIP(SessionInitiationProtocol) y H.323 para la señalización y para la transmisión de datos del protocolo RTP(Real Time Protocol), específicamente el protocolo SIP(SessionInitiationProtocol) y RTP(Real Time Protocol), son protocolos poco seguros, debido a que envían la información en texto plano, lo que supone un gran problema que afecta la confidencialidad de las comunicaciones, en el caso que personas no

autorizadas pretendan realizar ataques como escuchas y/o grabaciones ilícitas.

1.2 SOLUCIÓN PROPUESTA

Podemos mejorar la seguridad y confianza de la red VoIP mediante la implementación de controles de seguridad para paliar la mayoría de riesgos y ataques informáticos, entre algunos de los controles están:

- Mantener los sistemas actualizados y parcheados.
- Implementar protocolos de cifrado, debido a que el cifrado es el proceso para volver ilegible información considerada importante. La información una vez cifrada sólo puede leerse aplicándole una clave, esta medida de seguridad permite almacenar o transferir información delicada, que no debería ser accesible a terceros.
- Protegerse de ataques de enumeración.
- Revisar Logs
- Contraseñas fuertes
- Desactivar funcionalidades innecesarias

En resumen los beneficios que ofrece esta solución para proteger la central VoIP son:

- Garantizar una mitigación en posibles intrusiones a la central VoIP
- Garantizar la disponibilidad, integridad y confidencialidad en las comunicaciones

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 CENTRAL VOIP SIN SEGURIDADES

A continuación se describirá el escenario de pruebas inicial:

CPU core i7, 6 Gigas RAM, 750 Gigas disco duro

3 Laptops, 1 Tablet, 1 Smartphone

Sofphone Blink, LS Phone, Zoiper

Configuración de la central IP PBX:

- Elastix versión 2.5
- Firewall desactivado
- Llamadas anónimas activadas
- Parámetro allowguest = yes

Configuración de Extensiones:

Número	Descripción	Contraseña	NAT activado	Llamadas Simultáneas
100	Ventas	ventas100	Sí	Ilimitadas
101	Contabilidad	contabilidad101	Sí	Ilimitadas
102	Recepción	recepcion102	Sí	Ilimitadas
103	Gerencia	gerencia103	Sí	Ilimitadas
104	Soporte	soporte104	Sí	Ilimitadas

Tabla 1. Detalle de Extensiones

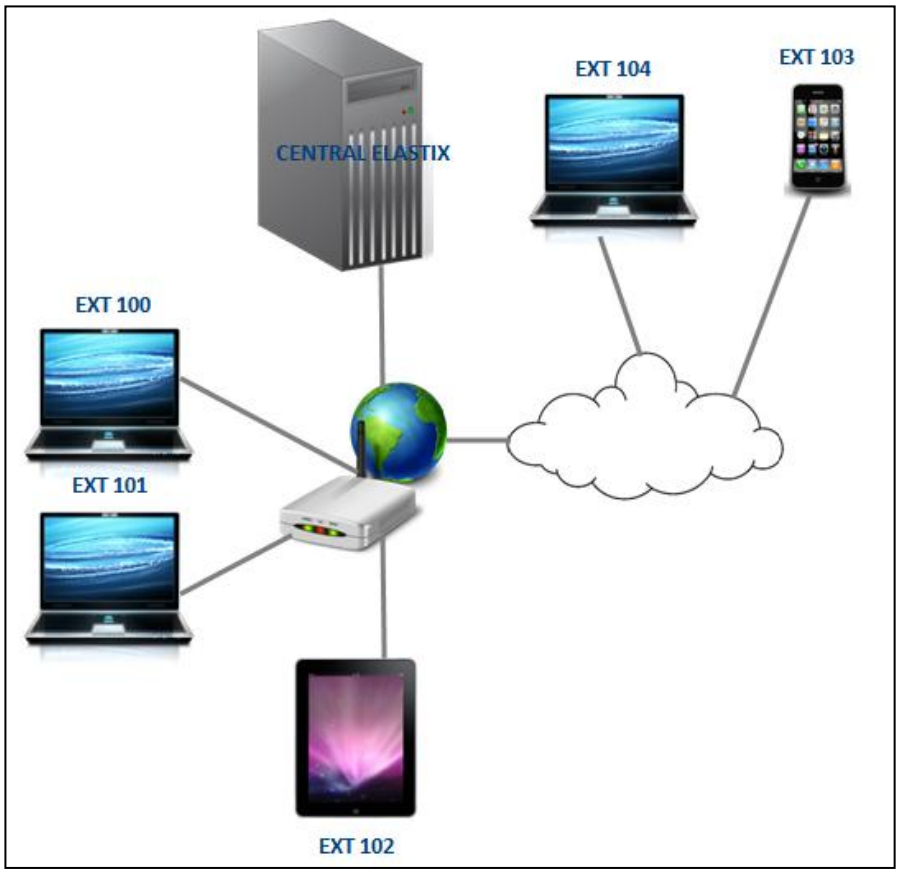


Figura 2.1 Esquema laboratorio infraestructura VoIP

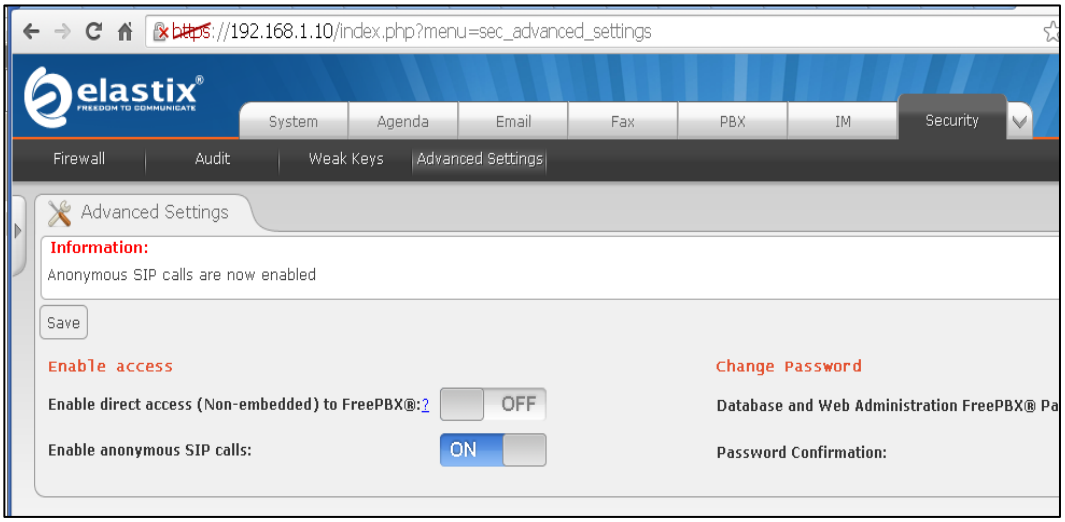


Figura 2.2 Llamadas anónimas activadas por defecto

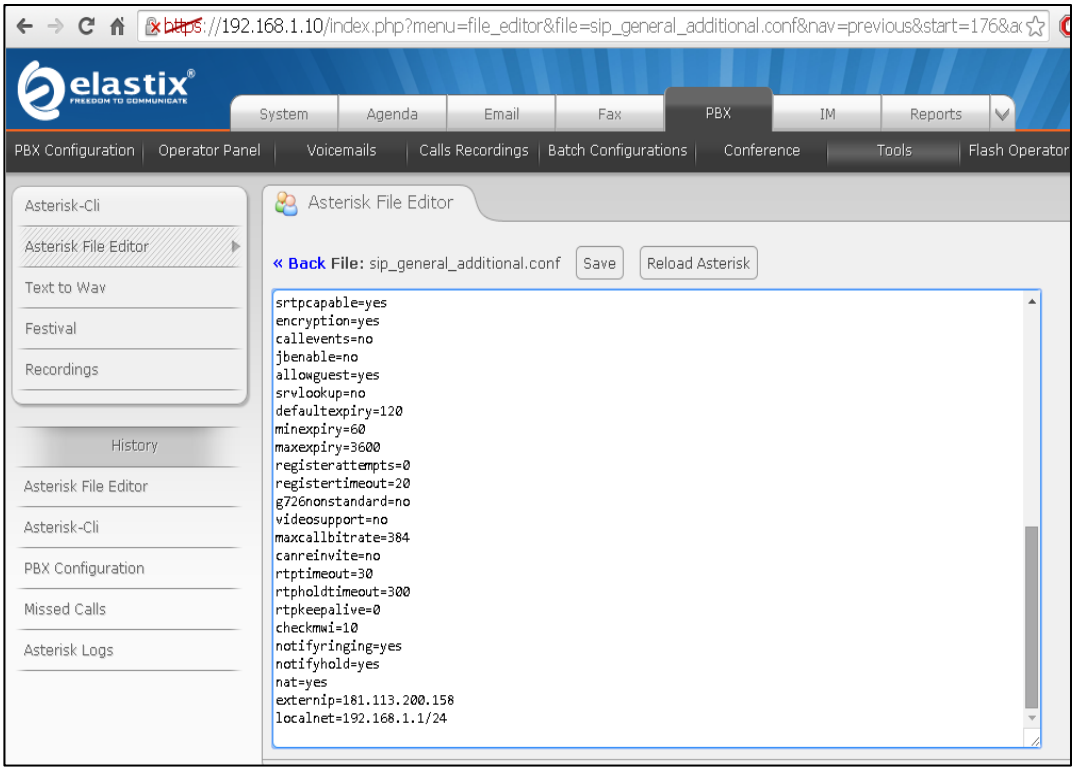


Figura 2.3 Parámetro allowguest

2.1.1 VECTORES DE ATAQUE INTERNOS

Los vectores de ataque internos serán ejecutados dentro de la red lan.

2.1.1.1 RECOPILACIÓN DE INFORMACIÓN

Varios métodos son utilizados para obtener información del sistema como versión del software, servidor, extensiones, servicios activos, etc. A continuación se detallan algunas herramientas que se pueden utilizar para obtener información del objetivo:

SipVicious: es un conjunto de herramientas usadas para auditar sistemas VoIP basados en SIP, consiste de 4 herramientas:

svmap- es un scanner SIP, lista dispositivos SIP encontrados en un rango de direcciones IP.

svwar-identifica extensiones activas en una IP PBX.

svcrack-crackea contraseñas en una IP PBX.

svreport-administra sesiones y exporta reportes en varios formatos.

svcrash-detiene escaneos no autorizados de herramientas svwar y svcrack [1].

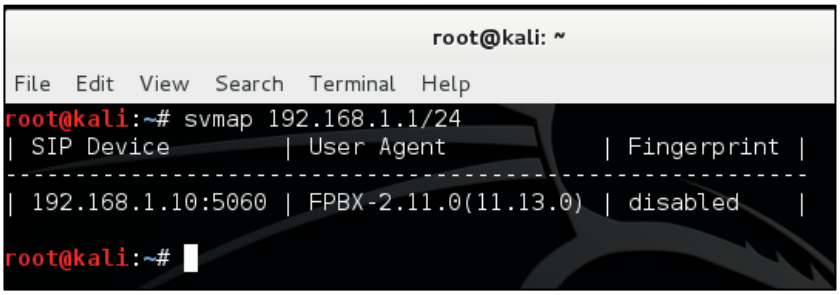


Figura 2.4 Resultado comando svmap

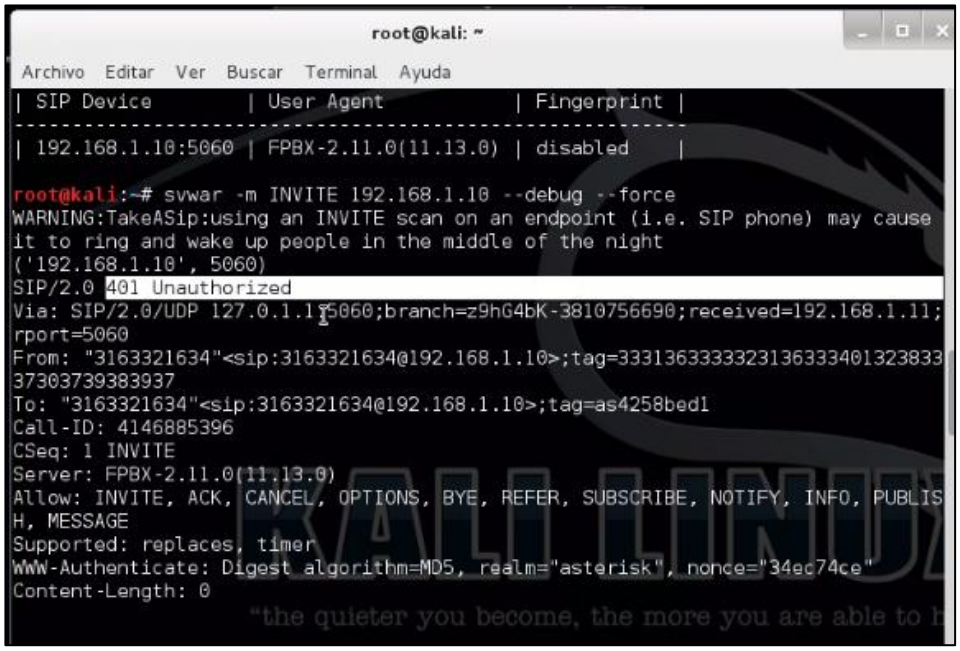


Figura 2.5 Salida comando svwar

Nmap: utilidad para la detección de redes y auditoría de seguridad. Nmap determina qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y versión), qué sistemas operativos (versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes /cortafuegos están en uso, y docenas de otras características [2].

#nmap –O 192.168.1.10

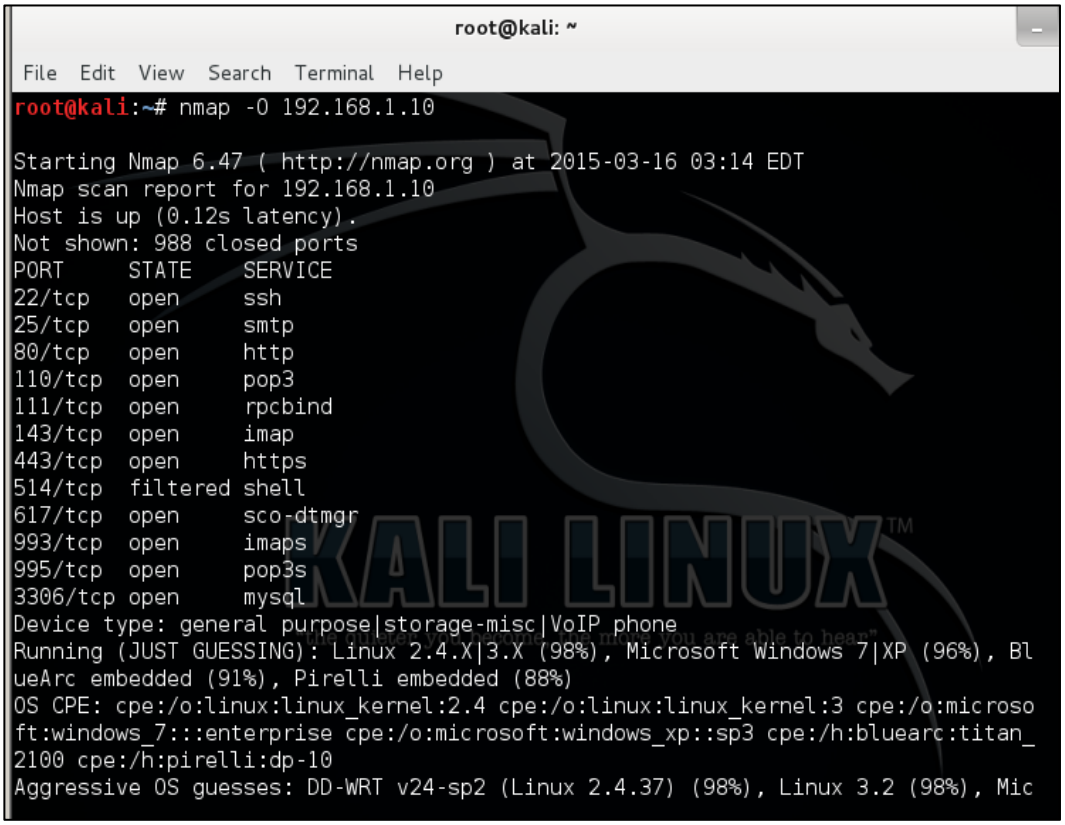


Figura 2.6 Salida comando nmap

Shodan: es un motor de búsqueda que permite al usuario buscar los dispositivos conectados a Internet. Los dispositivos se pueden encontrar en base a la ciudad, país, latitud / longitud, nombre de host, sistema operativo y la dirección IP. Shodan expone dispositivos potencialmente inseguros, y puede ser utilizado por atacantes para encontrar un sistema de VoIP sin protección, dispositivos VoIP sin autenticación, etc. [3].

Resultado: Con el comando svmap se logró obtener la dirección IP del servidor Elastix, con el comando svwar se logró obtener la enumeración de

las extensiones desde la 100 a la 104. Al escanear los puertos del servidor con la herramienta NMAP se obtuvieron 11 puertos abiertos, 1 filtrado.

2.1.1.2 ESCUCHA DE LLAMADAS EAVESDROP

Para escuchar una llamada en una red Voip, se realiza una captura de tráfico en la red y si la llamada no va cifrada se puede reproducir la conversación, una herramienta que se puede utilizar para la captura de tráfico se detalla a continuación:

Wireshark : es una herramienta que permite analizar protocolos en la red, puede capturar paquetes de datos viajando a través de la red, incluyendo SIP y otro tipo de paquetes VoIP, puede detectar automáticamente conversaciones VoIP [4].

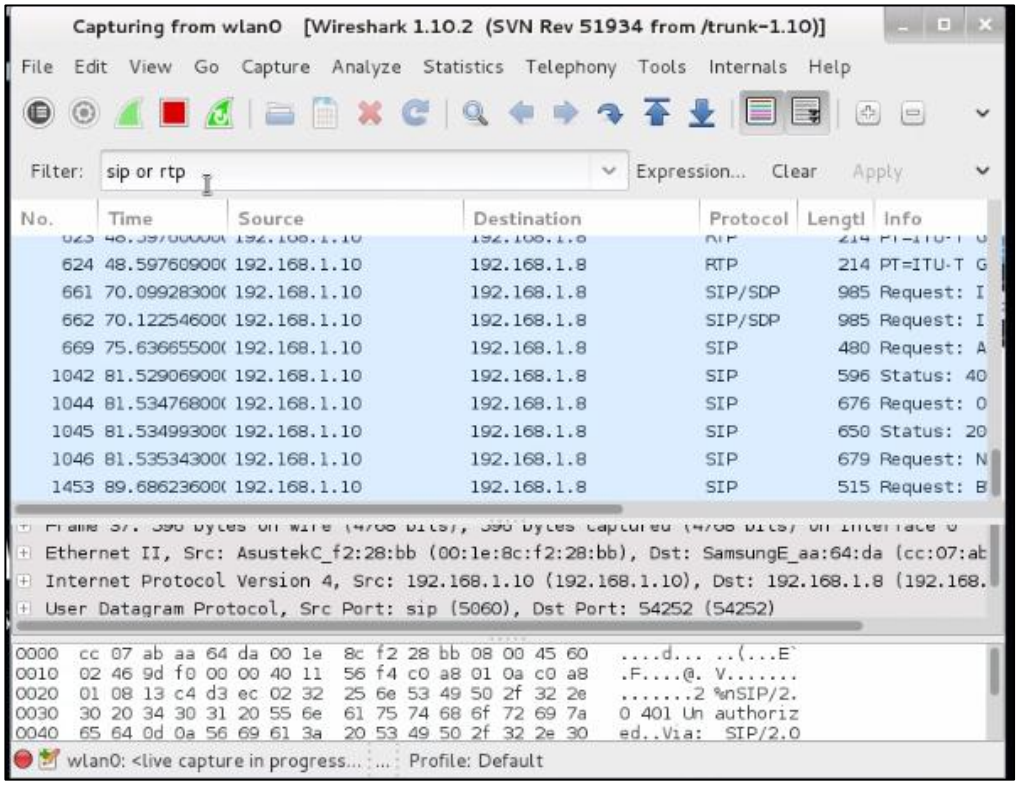


Figura 2.7 Captura de paquetes con Wireshark

Resultado: Fue posible realizar con Wireshark el esnifeo en la red y se logró reproducir luego la llamada, en el Apéndice 1 se puede ver como reproducir la llamada.

2.1.1.3 CRACKING DE CONTRASEÑAS

El protocolo SIP utiliza la autenticación digest para comprobar la identidad de sus clientes. El crackeo de la contraseña puede ser realizado con ataques de fuerza bruta, ataque de diccionario.

Se crackea los hashes digest de SIP con el fin de obtener el password de un usuario y poder utilizar la identidad de la víctima de forma maliciosa. Se detalla a continuación la herramienta utilizada:

SIPCrack: crackea las contraseñas del protocolo SIP en Linux, contiene dos herramientas:

sipdump: para esnifar los hashes de la autenticación .

sipcrack: para crackear los logins capturados [5].

Se ejcuta el comando para obtener los hashes de las autenticaciones:

#sipdump –i wlan0 /root/Desktop/captura.txt

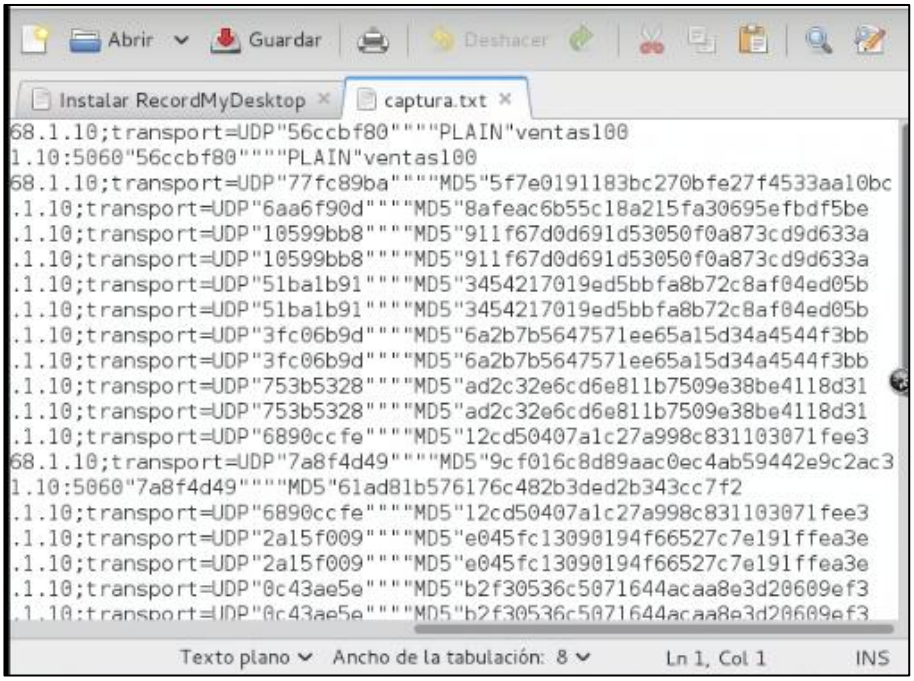


Figura 2.8 Archivo con hashes de autenticación digest

Una vez se tiene los hashes en el archivo captura.txt se intenta crackear los mismos utilizando un diccionario y el siguiente comando:

#sipcrack /root/Desktop/captura.txt –w /root/Desktop/diccionario2.lst

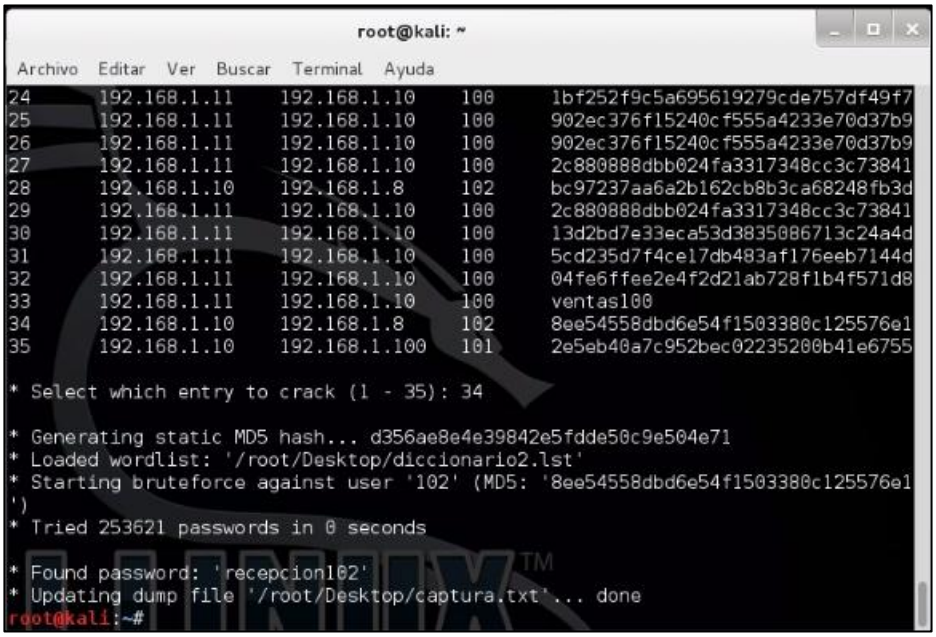


Figura 2.9 Salida comando sipcrack

Resultado: en la simulación realizada se logró crackear las claves de las extensiones 100, 101 y 102.

2.1.1.4 LLAMADAS FALSAS

Puede ser realizado, enviando una solicitud INVITE falsa, lo cual hace al dispositivo timbrar y mostrar en el identificador de llamadas una información falsa, a continuación se detalla un exploit utilizado para realizar esta tarea:

Inviteflood : permite manipular el campo From en una solicitud INVITE [6].

En la consola de Mestasploit

msf>use auxiliary/voip/sip_invite_spoof

msf>set DOMAIN 102@192.168.1.10

msf>set SRCADDR 120.120.120.120

msf>set MSG AUXILIO

msf>set RHOSTS 192.168.1.1/24

msf>set RPORT 62960

msf>run

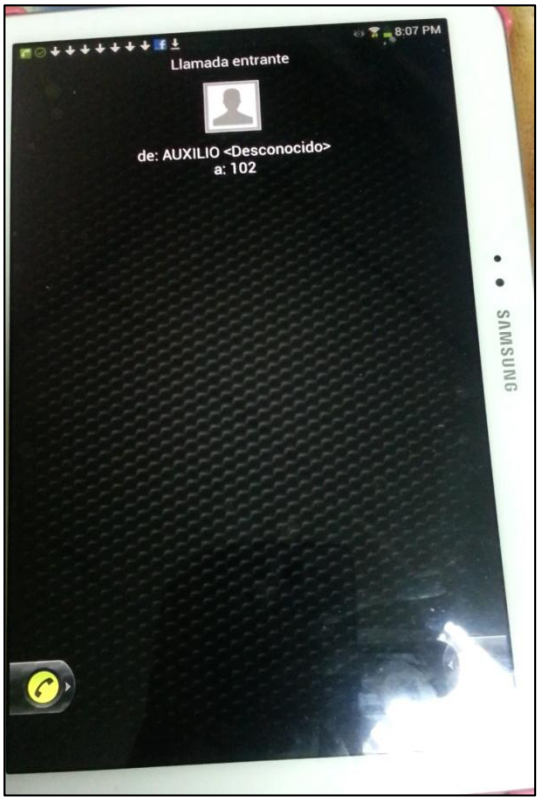


Figura 2.10 Ingreso de llamada falsa a extensión 102

Resultado: se logró realizar una llamada falsa con el campo from AUXILIO a la extensión 102.

2.1.1.5 INSERCIÓN DE AUDIO

RTP es un protocolo para la transmisión de datos, el cual hace a una comunicación VoIP vulnerable a ataques de inserción de audio. RTP es enviado en texto plano y se ejecuta sobre UDP. Un atacante puede capturar un paquete RTP y crear un paquete RTP similar al utilizado en la comunicación, pero con un mayor timestamp y número de secuencia, lo cual hace que el paquete original parezca antiguo, como el paquete tiene un válido SSRC (identificativo de la sesión actual), el paquete es aceptado como parte de la transmisión original [6].

Una herramienta para inserción de audio se detalla a continuación:

Rtpinsertsound: permite insertar un archivo de audio .wav a la conversación.

#rtpinsertsound –v –i wlan0 –b 192.168.1.8 –B 56752 –f 500 –j 50 /root/Downloads/prrueba.wav

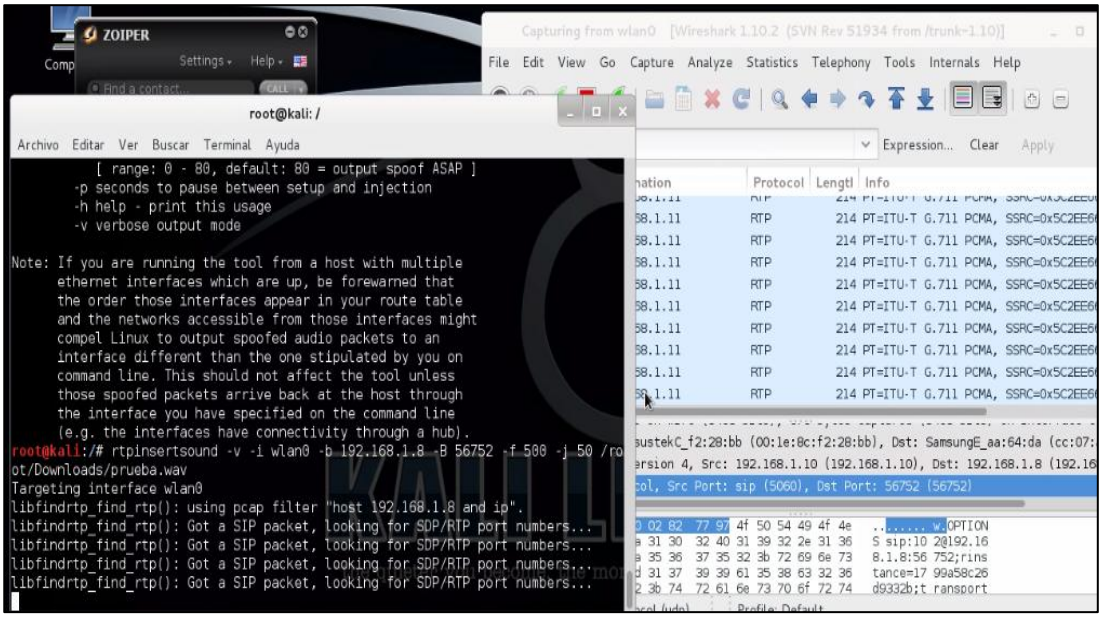


Figura 2.11 Salida comando rtpinsertsound

Resultado: no se logró escuchar el audio insertado, sin embargo tampoco se escuchaba el audio de la llamada.

2.1.1.6 ATAQUE DOS

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 construidos 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 [7].

A continuación se detalla una herramienta utilizada para un ataque DOS:

InviteFlood: inunda un objetivo con peticiones INVITE.

#inviteflood wlan0 102 192.168.1.10 192.168.1.100 300000 –a “DOS”

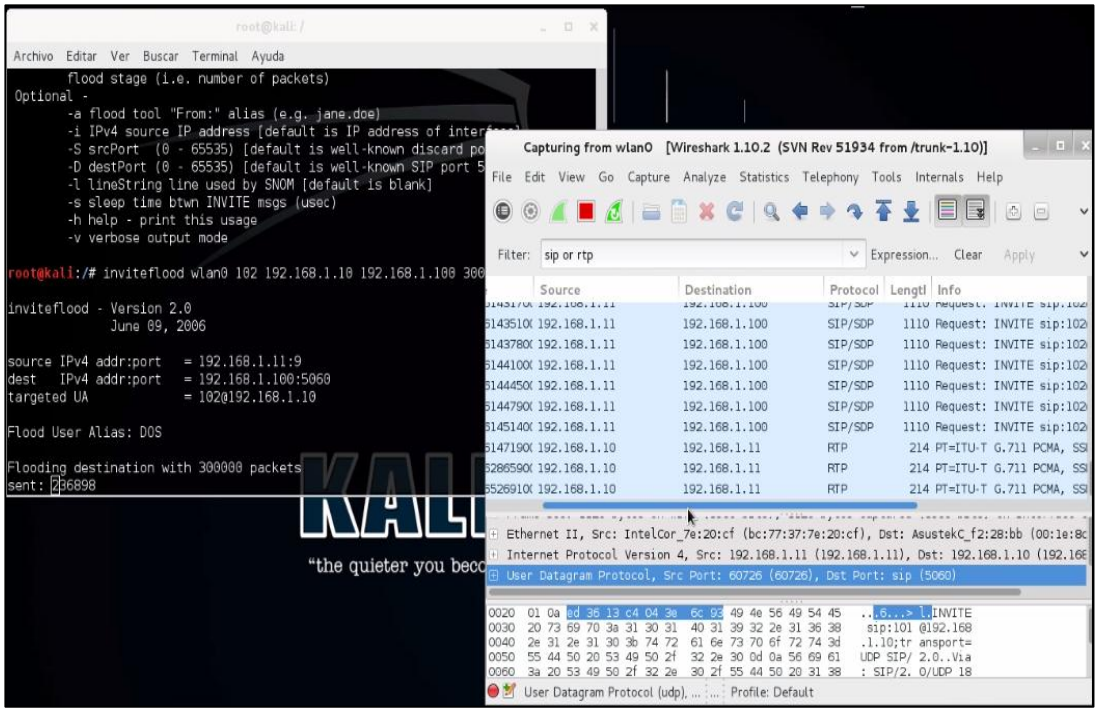


Figura 2.12 Salida comando inviteflood

Resultado: No se logró realizar una denegación de servicio en la conversación de la extensión 102.

2.1.2 VECTORES DE ATAQUE EXTERNOS

Se dejó expuesto el servidor Elastix, conectado al internet mediante NAT y los ataques que se detallan a continuación fueron detectados

2.1.2.1 REALIZAR LLAMADAS SIN AUTENTICACIÓN

No es necesario estar registrado para realizar una llamada. El comando REGISTER únicamente sirve para que nuestro servidor de VoIP sepa que estamos ahí y si llega una llamada destinada a nosotros, nos la pase. Es decir, nosotros nos registramos y le indicamos nuestros datos al servidor para que nos tenga localizados y sepa contactar con nosotros.

Por el contrario, a la hora de hacer una llamada, basta con enviar una petición (INVITE) [8].

En la página http://www.sinologic.net/proyectos/asterisk/checkSecurity/ verifican si el sistema permite el acceso desde el internet para realizar llamadas sin autenticación. Se realiza la prueba con la IP pública asignada en ese momento 181.196.154.199 para que realice la llamada a un número de Cuba(+53), se obtiene lo siguiente:

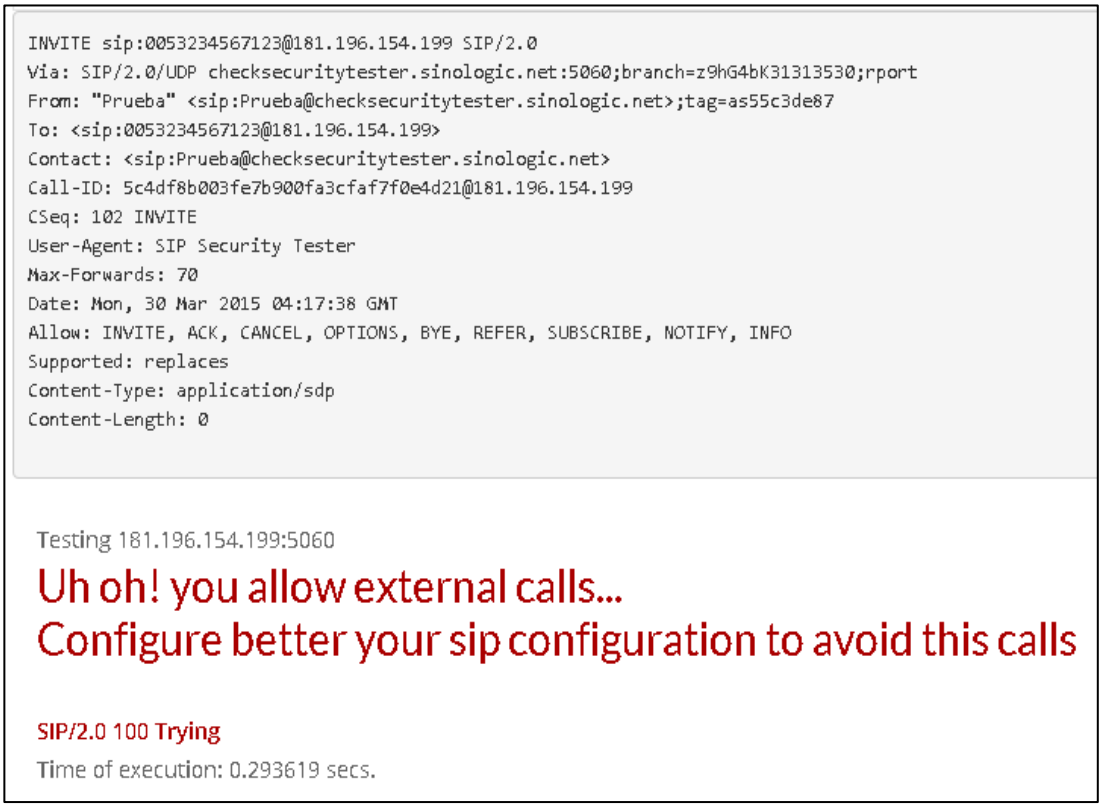


Figura 2.13 Resultado de verificación de llamadas anónimas

Además en el archivo /etc/log/asterisk/cdr-csv/Master.csv se observa que además personas no autorizadas realizaron llamadas con destinos 146, 147 y 1010 como se observa en la siguiente muestra:

EXTENSIÓN	E	TIPO	DESCRIPCIÓN				FECHA	SE	
53454657652	s	from-sip-external	"0053454657652"	SIP/checksecuritytester.sinologic.net	Congestion	5	3/22/2015 6:28	13	ANSWERED
146	s	from-sip-external	"146" <146>	SIP/181.196.231.13-00000012	Congestion	5	3/23/2015 2:08	13	ANSWERED
146	s	from-sip-external	"146" <146>	SIP/181.196.231.13-0000001e	Congestion	5	3/23/2015 3:11	13	ANSWERED
146	s	from-sip-external	"146" <146>	SIP/181.196.231.13-00000033	Congestion	5	3/23/2015 4:14	12	ANSWERED
146	s	from-sip-external	"146" <146>	SIP/181.196.231.13-00000034	Congestion	5	3/23/2015 5:18	12	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/181.196.231.13-00000035	Congestion	5	3/23/2015 5:28	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/181.196.231.13-00000036	Congestion	5	3/23/2015 6:17	13	ANSWERED
147	s	from-sip-external	"147" <147>	SIP/181.196.231.13-00000037	Congestion	5	3/23/2015 6:22	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/181.196.231.13-00000038	Congestion	5	3/23/2015 7:06	12	ANSWERED
147	s	from-sip-external	"147" <147>	SIP/181.196.231.13-00000039	Congestion	5	3/23/2015 7:26	12	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/181.196.231.13-0000003a	Congestion	5	3/23/2015 7:55	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000057	Congestion	5	3/25/2015 5:12	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000058	Congestion	5	3/25/2015 5:13	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000059	Congestion	5	3/25/2015 5:16	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-0000005a	Congestion	5	3/25/2015 5:19	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-0000005b	Congestion	5	3/25/2015 5:21	12	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-0000005c	Congestion	5	3/25/2015 5:24	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-0000005d	Congestion	5	3/25/2015 5:27	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-0000005e	Congestion	5	3/25/2015 5:30	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-0000005f	Congestion	5	3/25/2015 5:33	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000060	Congestion	5	3/25/2015 5:35	13	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000061	Congestion	5	3/25/2015 5:38	12	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000062	Congestion	5	3/25/2015 5:41	12	ANSWERED
1010	s	from-sip-external	"1010" <1010>	SIP/186.178.201.205-00000063	Congestion	5	3/25/2015 5:44	13	ANSWERED

Figura 2.14 Logs de /etc/log/asterisk/cdr-csv/Master.csv

A continuación se resume el número de llamadas realizadas :

DESTINO	3/22/2015	3/23/2015	3/25/2015	TOTAL
146	0	4	0	4
147	0	2	0	2
1010	0	4	211	215
53454657652	1	0	0	1
TOTAL	**1**	**10**	**211**	**222**

Tabla 2. Llamadas anónimas realizadas

Resultado: el servidor Elastix con la configuración por defecto es vulnerable a peticiones SIP INVITE sin autenticación.

2.1.2.2 ATAQUE A LA INTERFAZ WEB

Nivel de Sistema

El acceso a nivel de sistema implica el acceso al mismo sistema operativo, en última instancia mediante un terminal remoto.

Estos accesos se logran a través de algún servicio mal configurado, o de aplicaciones vulnerables que permitan la ejecución de código arbitrario en el server. Por ejemplo: si tenemos abierto un servicio telnet, o un SSH vulnerable, estamos dando al atacante una terminal de acceso para que simplemente comience a trabajar en su próximo paso : la escalada de privilegios.

Otra posible entrada a un sistema es la explotación de servicios vulnerables que permitan desbordamientos de búfers (que nos permitan, aún sin tener un terminal, ejecutar comandos en el sistema operativo).

Nivel de Aplicación

Los ataques a nivel de aplicación son aquellos que se realizan explotando vulnerabilidades de aplicaciones que permitan modificar los datos que la propia aplicación manipula, pero sin la posibilidad de

ejecución de comandos sobre el sistema operativo. Ejemplos: la modificación o borrado de contenidos en un sistema de gestión de portales, como phpNuke o Mambo. O la manipulación de una base de datos SQL mediante un acceso no autorizado a un phpMyAdmin vulnerable.

En este tipo de ataques el intruso puede cambiar lo que desee en nuestro sitio web, o en nuestras bases de datos. Pero no se puede considerar que el servidor esté comprometido, ni que el intruso haya entrado efectivamente en el sistema [9].

A continuación se resume las peticiones más relevantes realizadas que se encuentran en el log de httpd

IP	FECHA	PETICION	STATUS	DESCRIP	ISP	PAIS
217.112.97.187	[24/Mar/2015	GET /vtigercrm/ HTTP/1.1	404	NO ENCONTRADO	DTS-AS DIGITAL TE	ITALIA
198.20.69.74	[25/Mar/2015	GET /robots.txt HTTP/1.1	200	OK	SINGLEHOP-INC - S	USA
198.20.69.74	[25/Mar/2015	quit	200	OK	SINGLEHOP-INC - S	USA
207.244.83.130	[25/Mar/2015	GET /vtigercrm/test/upload/vtigercrm.txt HTTP/1.1	404	NO ENCONTRADO	LEASEWEB-US - Le	USA
188.138.1.218	[26/Mar/2015	GET /robots.txt HTTP/1.1	200	OK	PLUSSERVER-AS F	ALEMANIA
188.138.1.218	[26/Mar/2015	quit	200	OK	PLUSSERVER-AS F	ALEMANIA
217.112.97.187	[27/Mar/2015	GET /vtigercrm/ HTTP/1.1	404	NO ENCONTRADO	DTS-AS DIGITAL TE	ITALIA
117.37.36.118	[27/Mar/2015	GET /admin/config.php HTTP/1.1	200	OK	CHINANET-BACKB	CHINA
198.20.69.74	[27/Mar/2015	GET /robots.txt HTTP/1.1	200	OK	SINGLEHOP-INC - S	USA
198.20.69.74	[27/Mar/2015	quit	200	OK	SINGLEHOP-INC - S	USA
64.14.99.254	[28/Mar/2015	GET /vtigercrm/ HTTP/1.1	404	NO ENCONTRADO	SAVVIS - Savvis,US	USA
198.20.69.74	[28/Mar/2015	GET /robots.txt HTTP/1.1	200	OK	SINGLEHOP-INC - S	USA
198.20.69.74	[28/Mar/2015	quit	200	OK	SINGLEHOP-INC - S	USA

Figura 2.15 Logs de /var/log/httpd

En las peticiones GET /vtigercrm/ HTTP/1.1 y GET /vtigercrm/test/upload/vtigercrm.txt HTTP/1.1 quisieron atacar

vulnerabilidades en software de terceros, en este caso VTIGER, para revisar sobre esta vulnerabilidad [10].

A continuación se muestran los resultados de estas peticiones:

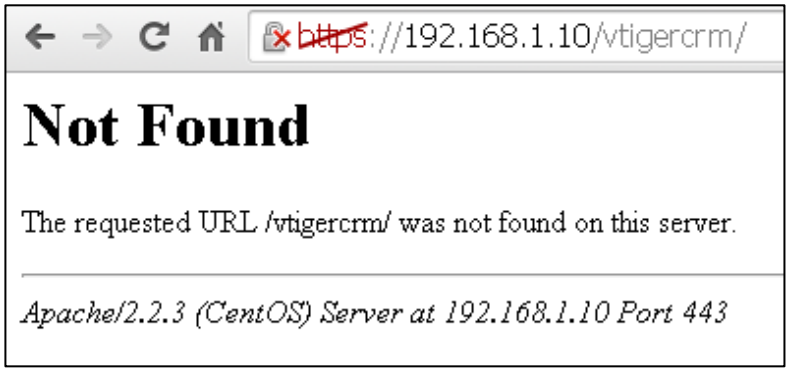


Figura 2.16 Petición Get /vtigercrm/

Figura 2.17 Petición Get /vtigercrm/test/upload/vtigercrm.txt

Con la petición GET /robots.txt HTTP/1.1 visualizaron el contenido del archivo robots.txt

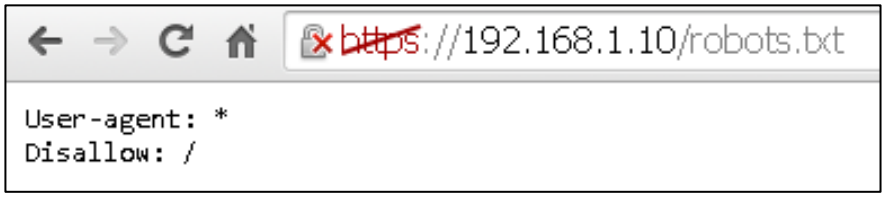


Figura 2.18 Petición Get /robots.txt

Con la petición GET /admin/config.php HTTP/1.1 quisieron atacar la vulnerabilidad de FreePBX, para revisar sobre esta vulnerabilidad [11].

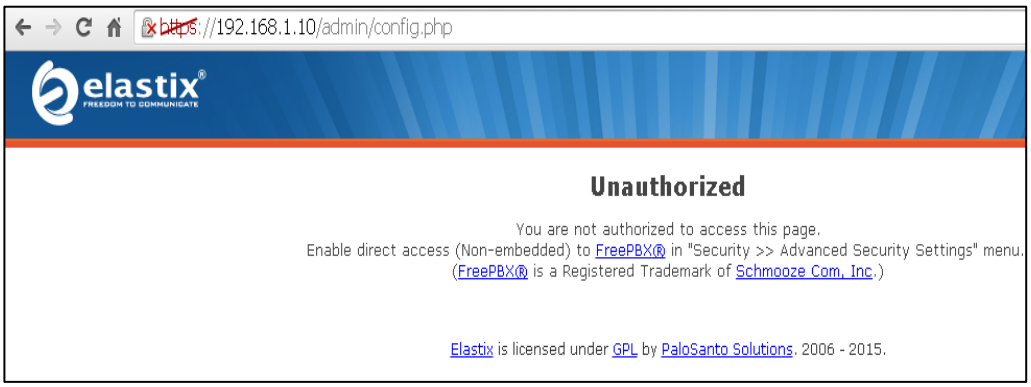


Figura 2.19 Petición Get /admin/config.php

Resultado: Intentaron realizar algunos ataques a través del servidor web, sin embargo no fueron exitosos, pero lograron recopilar información como el tipo de servidor web, la versión, el puerto utilizado para https. En el Apéndice 2 se puede observar el detalle de los logs.

2.2 IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

Se tratará de mitigar las vulnerabilidades encontradas para evitar intrusiones no autorizadas.

2.2.1 CIFRADO

A nivel de señalización para el cifrado se utilizará TLS y para la media se utilizará SRTP. En cada extensión se escoge las siguientes opciones para habilitar el cifrado:

Transport: TLS Only

Encryption: Yes(SRTP only)

Se generan certificados para el servidor y para las extensiones.

Para una guía más detallada se encuentra en las referencias [12].

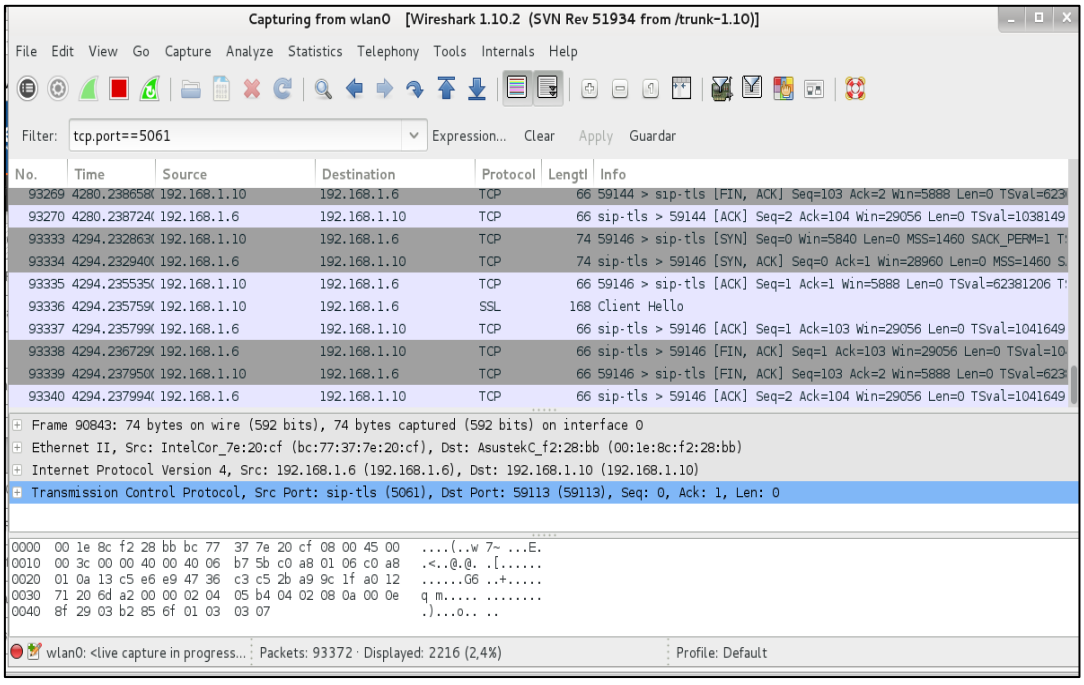


Figura 2.20 Captura de señalización TLS

2.2.2 HARDENING DE ELASTIX

La mayoría de recomendaciones han sido seguidas de la guía de Samuel Cornu [13].

Desactivar Llamadas Anónimas

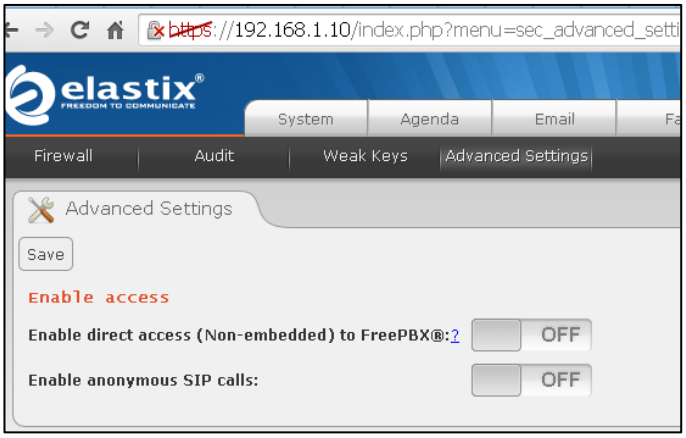


Figura 2.21 Llamadas anónimas desactivadas

Una vez desactivadas las llamadas anónimas que permiten recibir peticiones INVITE sin autenticación se probó si era posible realizar llamadas desde internet y este fue el resultado:

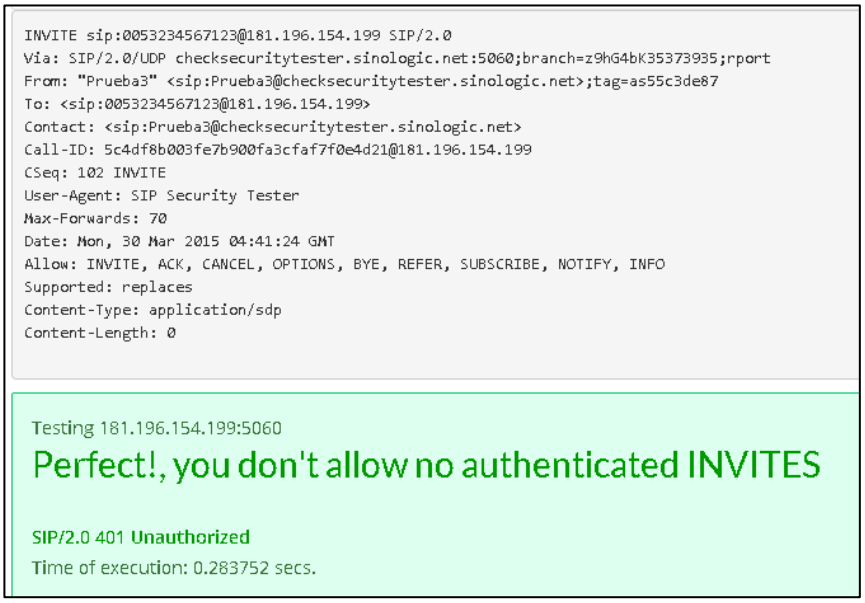


Figura 2.22 Resultado de verificación de llamadas anónimas

Desactivación de Servicios Innecesarios

Se desactivan los 8 servicios que se muestran a continuación:

	SERVICIOS
1	IP6TABLES
2	NETFS
3	NFSLOCK
4	PORTMAP
5	RESTORECOND
6	RPCGSSD / RPCIDMAPD
7	WANROUTER
8	XINETD

Tabla 3. Servicios desactivados en central Elastix

Para el detalle de la descripción y los comandos utilizados para desactivar los servicios descritos ver Apéndice 3.

Asegurar SSH

SSH (Secure Shell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos.

1.-Crear un usuario y asignarlo al grupo Wheel, con lo cual solo ese usuario podrá hacer uso del comando su, el cual permite convertirse en superusuario. Ver Apéndice 4

2.- Usar contraseñas Fuertes

Con contraseñas fuertes cualquier ataque será registrado y notificado antes de que pueda tener éxito. Escoger combinaciones que cumplan las siguientes particularidades:

- 12 Caracteres como mínimo
- Mezclar letras mayúsculas y minúsculas
- Mezclar letras y números

- Usar caracteres no alfabéticos (ej.: caracteres especiales como ! " £ $ % ^ etc.)
- Rotar las contraseñas periódicamente.

3.- Deshabilitar el acceso como root

La configuración del servidor SSH se encuentra almacenada en el fichero /etc/ssh/sshd_config. Para deshabilitar el acceso de root:

Authentication:

#LoginGraceTime 2

PermitRootLogin no

Reiniciar el servicio sshd:

servicesshdrestart

Si se necesita acceder como root, se accede como un usuario normal que pertenezca al grupo Wheel y se usa el comando su.

4. No utilizar el puerto por defecto

Por defecto, SSH escucha las conexiones entrantes en el puerto 22. Es mejor escoger cualquier puerto alto al azar que no sea usado por ningún servicio conocido, pero es preferible usar uno por encima del 1024.

Para hacer los cambios, se añade una línea como esta al fichero /etc/ssh/sshd_config:

Ejecutar ssh en un puerto No-Estándar:

Port 37037

Reiniciar el servicio sshd.

servicesshdrestart

Activar el Firewall de Elastix

Se activa el firewall para que los servicios ssh, http y https solo se puedan acceder desde la ip 192.168.1.6.Para ver más detalle Apéndice 5.

Utilizar Fail2ban

Fail2Ban es un analizador de logs que busca intentos fallidos de registro y bloquea las IP’s de donde provienen estos intentos. Se distribuye bajo la

licencia GNU y típicamente funciona en todos los sistemas que tengan interfaz con un sistema de control de paquetes o un firewall local.

Fail2Ban tiene una gran configuración pudiendo, además, crear reglas para programas propios o de terceros.

En Elastix 2.5 ya viene instalado por lo que se debe configurar y activar. Ver Apéndice 6.

Asegurar Https

Hay que configurar Apache para que antes de que autentifique Elastix tome algunos recaudos de seguridad mediante htpasswd. Editar el archivo /etc/httpd/conf.d/elastix.conf. Ver Apéndice 7.

El servidor de contenidos web mostrará una ventana en lugar de la página de inicio de Elastix. Todo intento de acceso erróneo será guardado en los archivos de log que se encuentran en /var/log/httpd/

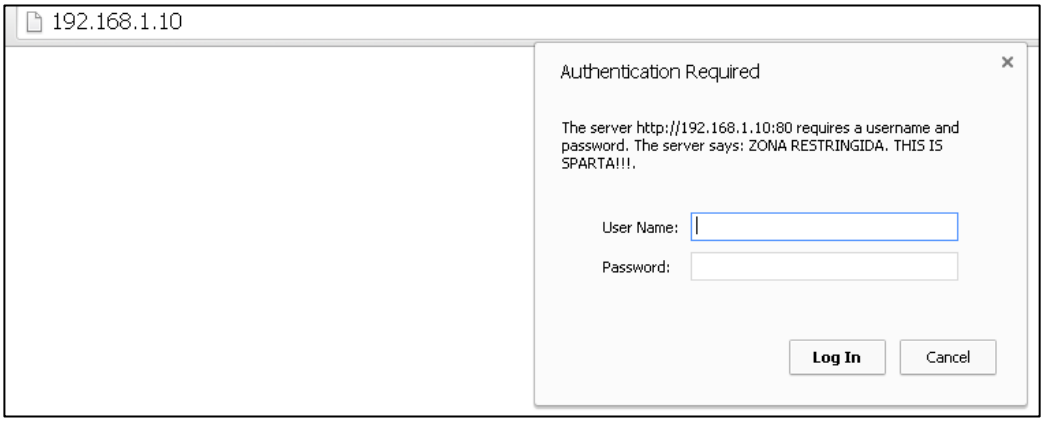


Figura 2.23 Ventana de petición de usuario y contraseña

Seguridad en las extensiones

- Desactivación de Nat en las extensiones que no son remotas.
- Robustez de las contraseñas

Número	Descripción	Contraseña	NAT activado	Llamadas Simultáneas
100	Ventas	sT7Ñv$4c8Cm/dm*Mt0aVd	No	2
101	Contabilidad	F7&ysw)PqÑ4gcK$hxiL8y	No	2
102	Recepción	gH9wl(Do*xnlsWÑb30sHe	No	2
103	Gerencia	Uysw3%Tdi0=ÑvzjoA9YdZ1	Sí	2
104	Soporte	hñf5=S8Ghxlu0C/RhyJ3$	Sí	2

Tabla 4. Extensiones con contraseñas cambiadas

Evitar recopilación de información

Para evitar que se muestra la versión de apache se edita el archivo httpd.conf que se encuentra en la ruta /etc/httpd/conf/:

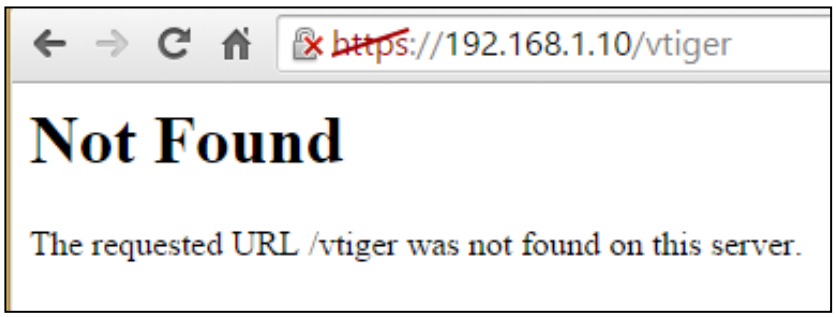


Figura 2.24 Petición Get /vtiger sin mostrar datos

Para evitar que se realice escaneo y enumeración de extensiones se configura lo mostrado en el Apéndice 8.

Resultado: Se logró evitar que se muestre la versión de Apache y el tipo de central, sin embargo no se logró evitar el descubrimiento de la dirección ip del servidor Elastix, enumeración de extensiones y escaneo de puertos.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 DISPONIBILIDAD EN LA COMUNICACIÓN

La disponibilidad es garantizar que el servicio de la comunicación esté disponible cuando se necesite. En los escenarios planteados en este trabajo, existieron tres vectores de ataque que pueden comprometer la disponibilidad en el servicio de comunicación, se muestran a continuación:

Disponibilidad	
Vector de Ataque	**Afectación**
Ataque DoS	No
Realizar Llamadas sin Autenticación	Si
Ataque a la Interfaz Web	No

Tabla 5. Afectación de vectores de ataque a la disponibilidad

Figura 3.1 Afectación en la disponibilidad

La contramedida para solucionar que se realicen llamadas a través de la central Elastix sin autenticación, fue desactivar las llamadas anónimas, con lo cual se logró una mitigación del 100%.

3.2 INTEGRIDAD EN LA COMUNICACIÓN

La integridad es garantizar que la información que se transmite en el servicio de la comunicación sólo puede ser modificada por personas autorizadas. En los escenarios planteados en este trabajo, existieron tres vectores de ataque que pueden comprometer la integridad en el servicio de comunicación, se muestran a continuación:

Integridad	
Vector de Ataque	**Afectación**
Llamadas Falsas	Si
Inserción de Audio	Si
Ataque a la Interfaz Web	No

Tabla 6. Afectación de vectores de ataque a la integridad

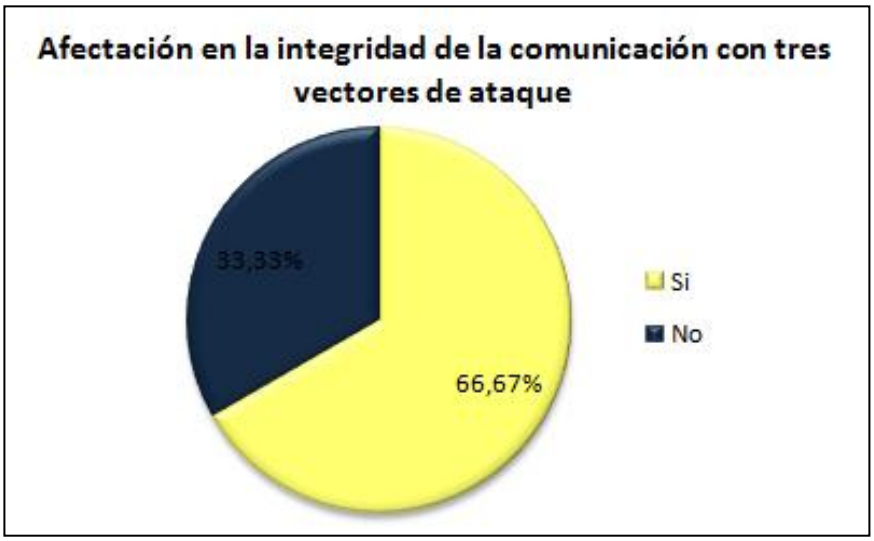


Figura 3.2 Afectación en la integridad

La contramedida para solucionar que se realicen llamadas falsas e inserción de audio a través de la central Elastix, fue implementar el cifrado en la señalización y voz, con lo cual se logró una mitigación del 100%.

3.3 CONFIDENCIALIDAD EN LA COMUNICACIÓN

La confidencialidad es garantizar que la información que se transmite en el servicio de la comunicación sólo puede ser legible y/o escuchada por personas autorizadas. En los escenarios planteados en este trabajo, existieron cuatro vectores de ataque que pueden comprometer la confidencialidad en el servicio de comunicación, se muestran a continuación:

Confidencialidad	
Vector de Ataque	**Afectación**
Recopilación de Información	Si
Escucha de llamadas	Si
Cracking de contraseñas	Si
Ataque a la Interfaz Web	No

Tabla 7. Afectación de vectores de ataque a la confidencialidad

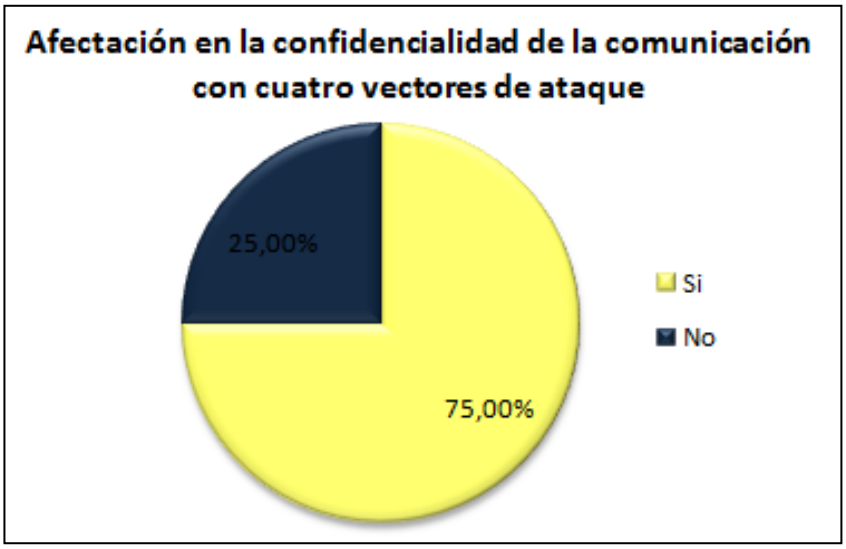


Figura 3.3 Afectación en la confidencialidad

La contramedida para solucionar que se realice una recopilación de información de la central Elastix, fue configurar archivos como httpd.conf y sip_general_additional.conf para que no muestren información, con lo cual se logró una mitigación del 33%.

La contramedida para solucionar que se realicen escucha de llamadas durante una conversación, fue implementar el cifrado en la señalización y voz, con lo cual se logró una mitigación del 100%.

La contramedida para solucionar que se realice un cracking de contraseñas , fue activar un servicio que bloquee a una dirección IP luego de 3 intentos de autenticación fallidos en la central Elastix, con lo cual se logró una mitigación del 97%.

CONCLUSIONES

1. La disponibilidad del servicio de la comunicación fue afectada en un 33% con el vector de ataque "Realizar llamadas sin autenticación", lo cual fue producto de haber dejado la central Elastix con la configuración por defecto en la cual permitía realizar llamadas anónimas, es decir sin autenticarse en la central Elastix, sin embargo se logró mitigar la afectación en un 100% con la desactivación de las llamadas anónimas en la central Elastix.
2. La integridad de la información que se transmite en el servicio de la comunicación fue afectada en un 66,67% con los vector de ataque "Llamadas Falsas" e "Inserción de Audio", lo cual se debió a que la señalización y la voz iban en texto plano, sin embargo se logró mitigar la afectación en un 100% con la implementación de cifrado en la central Elastix, se utilizó TLS para la señalización y SRTP para la voz.

3. La confidencialidad de la información que se transmite en el servicio de la comunicación fue afectada en un 75% con los vectores de ataque "Recopilación de Información", "Escucha de Llamadas" y "Cracking de Contraseñas", lo cual fue resultado de configuraciones por defecto, que la señalización y la voz iban en texto plano, no había un servicio de bloqueo para direcciones IP que fallaran en la autenticación, sin embargo se logró mitigar la afectación en un 33% del vector de ataque "Recopilación de Información" con la configuración de archivos como httpd.conf y sip_general_additional.conf para que no muestren información, 100% del vector de ataque "Escucha de Llamadas" con la implementación de cifrado en la central Elastix, se utilizó TLS para la señalización y SRTP para la voz, 97% del vector de ataque " Cracking de Contraseñas " con la activación del servicio para bloquear una dirección IP luego de 3 intentos de autenticación fallidos, que es fail2ban, en la central Elastix.
4. Se implementaron otras medidas como robustez en las contraseñas, extensiones que permitan solo dos llamadas simultáneas, acceso dedicado a servicios de alto riesgo como ssh, https a través de iptables para mitigar posibles ataques que comprometan al servidor Elastix.

RECOMENDACIONES

1. Desarrollar una política de seguridad que sea una herramienta organizacional para concienciar a los trabajadores de la empresa sobre la importancia y sensibilidad de la información y servicios críticos que entre sus objetivos tenga evitar fuga de Información por parte de los empleados, administradores de redes y/o personal de manteniendo, que realizan un mal uso de la información compartiendo las contraseñas y accesos, ya que de nada serviría implementar los mejores mecanismos de seguridad.

2. Estar al día en actualizaciones, vulnerabilidades y soluciones, ya que con el avance tecnológico seguirán apareciendo vulnerabilidades, la seguridad es un proceso constante e iterativo, el cual requiere tener la importancia adecuada para minimizar los riesgos de ataques que afecten a la empresa económicamente, en su funcionamiento o a su imagen.

BIBLIOGRAFÍA

[1]. Google Project Hosting, sipvicious, https://code.google.com/p/sipvicious/, fecha de consulta marzo 2015

[2]. Insecure.Org, Introduccion Nmap, http://nmap.org/, fecha de consulta marzo 2015

[3]. SHODAN, shodan, https://www.shodan.io/, fecha de consulta marzo 2015

[4]. Wireshark Foundation, Acerca de Wireshark, https://www.wireshark.org /about.html, fecha de consulta marzo 2015

[5]. Ubuntu Manpage Repository, sipcrack, http://manpages.ubuntu.com/ manpages/precise/man1/sipcrack.1.html, fecha de consulta marzo 2015

[6]. Endler David and Collier Mark, Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions, McGraw-Hill/Osborne, 2007

[7]. (Bud) Bates, Regis J. Jr, Securing VoIP: Keeping Your VoIP Network Safe, Syngress, 2014

[8]. Sinologic Network, SIPCheck: Vigila quien intenta registrarse en tu Asterisk,https://www.sinologic.net/blog/2010-05/sipcheck-vigila-quien- intenta-registrarse -en-tu-asterisk.html, fecha de consulta marzo 2015

[9]. EC-Council, Ethical Hacking and Countermeasures: Web Applications and Data Servers (EC-Council Press), Cengage Learning, 2009

[10]. Oliva Juan, Explotando Vulnerabilidad php code injection exploit en vtiger 5.2.1,https://jroliva.wordpress.com/2013/06/17/explotando-vulnerabilidad-php-code-inyection-en-vtiger-5-2-1/, fecha de consulta marzo 2015

[11]. Oliva Juan, Probando Vulnerabilidad en Elastix (backdoor freebx),https://jroliva.wordpress.com/2011/05/30/probando-vulnerabilidad-en-elastix-backdoor -freebx/, fecha de consulta marzo 2015

[12]. Almeida Juan, SIP TLS y SRTP en Elastix, http://juanelojga.blogspot.com/ 2012/07/sip-tls-y-srtp-en-elastix.html, fecha de consulta marzo 2015

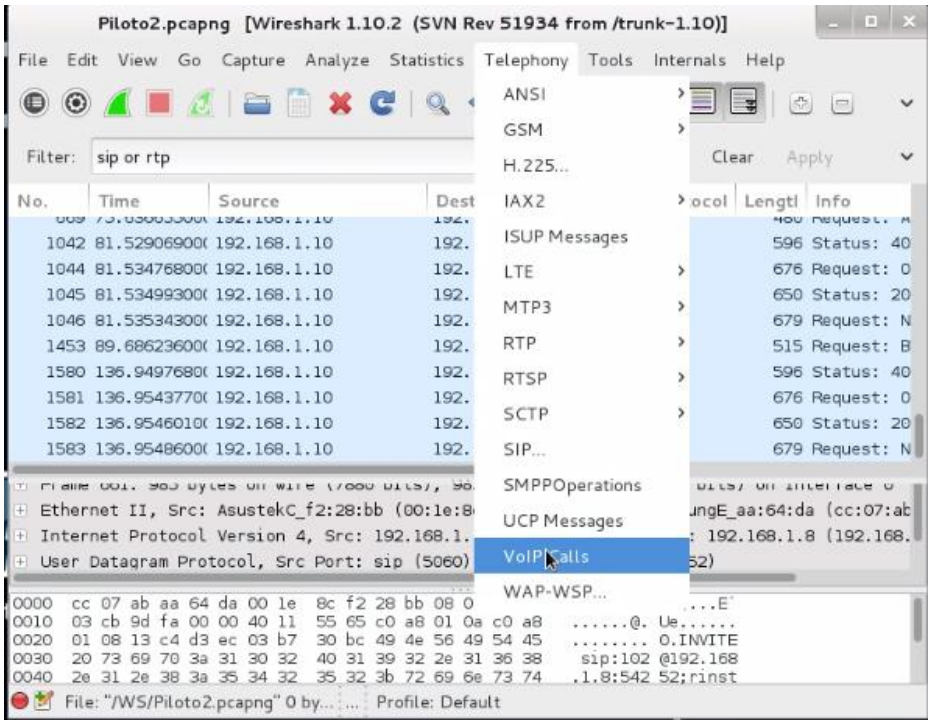
[13]. Samuel Cornu, Asegurando Elastix, http://sourceforge.net/projects/elastix/files/Tutorials_Docs_Manuals/Third%20Party%20Documentation/Security/Asegurando%20Elastix%20%20Samuel%20Cornu.pdf/download, fecha de consulta marzo 2015

[14]. Oliva Juan, Módulo de Seguridad en Elastix : Restringir el Acceso al Entorno Web,https://jroliva.wordpress.com/2012/07/02/modulo-de-seguridad-en-elastix-restringir-el-acceso-al-entrorno-web/, fecha de consulta marzo 2015

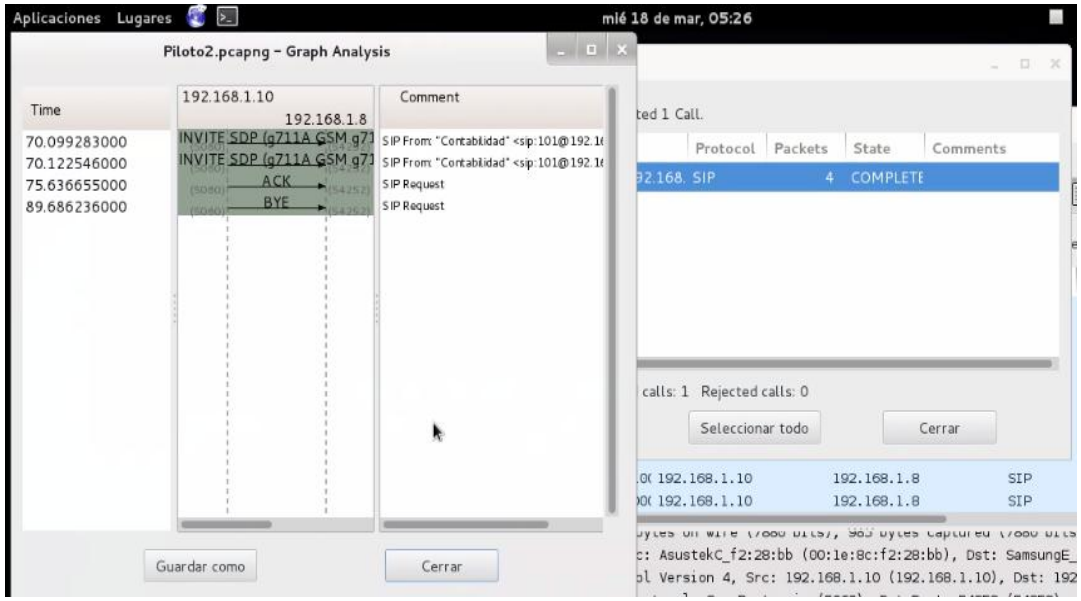
APÉNDICE

1.- REPRODUCIR UNA LLAMADA CON WIRESHARK

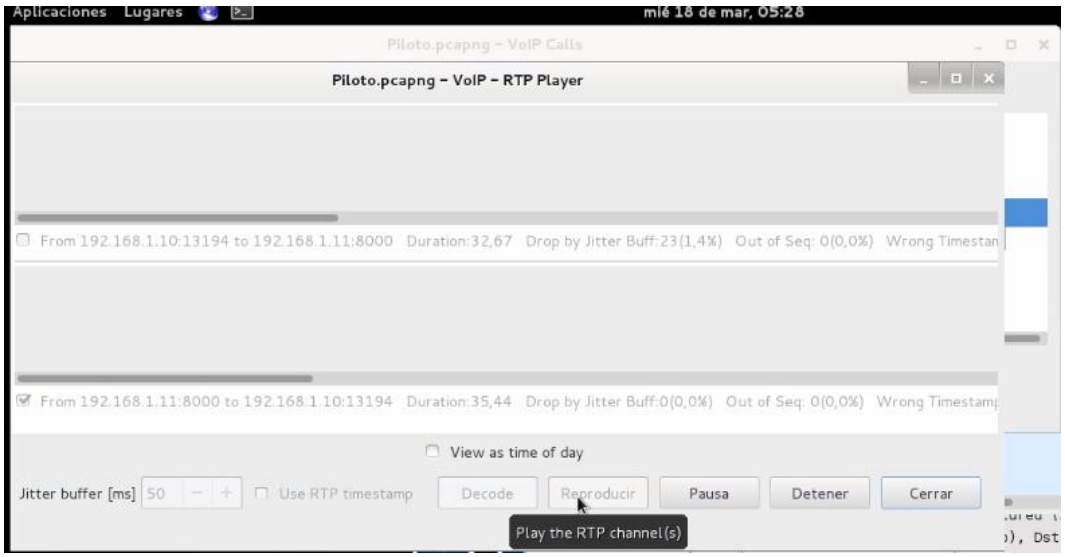
En el menú Telephony se escoge la opción VoIPCalls



Se da click en Flow y se puede ver detalles de la señalización de la llamada



Se da click en Player, luego Decode y finalmente en Reproducir



2.- LOGS HTTPS

IP	1	2	3	4	5	STATUS	6	ISP	PAIS
184.105.139.67	-	-	[22/Mar/2015:21:35:34	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
184.105.139.67	-	-	[22/Mar/2015:21:39:56	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
74.82.47.3	-	-	[24/Mar/2015:05:42:07	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
74.82.47.3	-	-	[24/Mar/2015:05:50:45	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
217.112.97.187	-	-	[24/Mar/2015:12:49:36	-0500]	GET /vtigercrm/ HTTP/1.1	404	288	DTS-AS DIGITAL TELECOMMUNIC	ITALIA
216.218.206.66	-	-	[25/Mar/2015:06:22:22	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
216.218.206.66	-	-	[25/Mar/2015:06:26:29	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
198.20.69.74	-	-	[25/Mar/2015:07:31:12	-0500]	GET / HTTP/1.1	200	2609	SINGLEHOP-INC - SingleHop	USA
198.20.69.74	-	-	[25/Mar/2015:07:31:15	-0500]	GET /robots.txt HTTP/1.1	200	28	SINGLEHOP-INC - SingleHop	USA
198.20.69.74	-	-	[25/Mar/2015:07:31:30	-0500]	quit	200	2609	SINGLEHOP-INC - SingleHop	USA
207.244.83.130	-	-	[25/Mar/2015:08:47:26	-0500]	GET /vtigercrm/test/upload/vtigercrm.txt HTTP/1.1	404	314	LEASEWEB-US - Leaseweb US	USA
207.244.83.130	-	-	[25/Mar/2015:10:13:29	-0500]	GET /	400	525	LEASEWEB-US - Leaseweb US	USA
207.244.83.130	-	-	[25/Mar/2015:10:13:29	-0500]	GET /	400	525	LEASEWEB-US - Leaseweb US	USA
74.82.47.2	-	-	[25/Mar/2015:23:20:39	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
74.82.47.2	-	-	[25/Mar/2015:23:27:10	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
188.138.1.218	-	-	[26/Mar/2015:02:17:18	-0500]	GET / HTTP/1.1	200	2609	PLUSSERVER-AS PlusServer A	ALEMANIA
188.138.1.218	-	-	[26/Mar/2015:02:17:19	-0500]	GET /robots.txt HTTP/1.1	200	28	PLUSSERVER-AS PlusServer A	ALEMANIA
188.138.1.218	-	-	[26/Mar/2015:02:17:31	-0500]	quit	200	2609	PLUSSERVER-AS PlusServer A	ALEMANIA
217.112.97.187	-	-	[27/Mar/2015:09:13:29	-0500]	GET /vtigercrm/ HTTP/1.1	404	288	DTS-AS DIGITAL TELECOMMUNIC	ITALIA
117.37.36.118	-	-	[27/Mar/2015:14:21:31	-0500]	GET /admin/config.php HTTP/1.1	200	1444	CHINANET-BACKBONE No.31,Ji	CHINA
198.20.69.74	-	-	[27/Mar/2015:22:48:29	-0500]	GET / HTTP/1.1	200	2609	SINGLEHOP-INC - SingleHop	USA
198.20.69.74	-	-	[27/Mar/2015:22:48:32	-0500]	GET /robots.txt HTTP/1.1	200	28	SINGLEHOP-INC - SingleHop	USA
198.20.69.74	-	-	[27/Mar/2015:22:48:47	-0500]	quit	200	2609	SINGLEHOP-INC - SingleHop	USA
64.14.99.254	-	-	[28/Mar/2015:01:15:09	-0500]	GET /vtigercrm/ HTTP/1.1	404	289	SAVVIS - Savvis,US	USA
184.105.247.195	-	-	[28/Mar/2015:02:14:35	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
184.105.247.195	-	-	[28/Mar/2015:02:16:44	-0500]	GET / HTTP/1.1	200	2609	HURRICANE - Hurricane Elec	USA
198.20.69.74	-	-	[28/Mar/2015:09:05:28	-0500]	GET / HTTP/1.1	200	2609	SINGLEHOP-INC - SingleHop	USA
198.20.69.74	-	-	[28/Mar/2015:09:05:29	-0500]	GET /robots.txt HTTP/1.1	200	28	SINGLEHOP-INC - SingleHop	USA
198.20.69.74	-	-	[28/Mar/2015:09:05:37	-0500]	quit	200	2609	SINGLEHOP-INC - SingleHop	USA

3.-DESACTIVACIÓN DE SERVICIOS INNECESARIOS

IP6TABLES Esta tarea se realiza ejecutando lo siguiente:

chkconfig –level 345 ip6tables off

NETFS Monta sistema de archivos en red como NFS, Samba, entre otros. Al momento del inicio del sistema. Para desactivar este servicio ejecutamos la siguiente acción:

chkconfig --level 345 netfs off

NFSLOCK Bloquea los archivos que se encuentran compartidos en la red a través de NFS. Si no utiliza NFS para acceder a unidades compartidas puede deshabilitar este servicio. Para desactivar este servicio ejecutamos la siguiente acción:

chkconfig –level 345 nfslock off

PORTMAP Es un Servicio complementario al NFS (Network File System) y NIS (Autenticación). Si no se hace uso de NFS, el servicio debe estar desactivado. Para desactivar este servicio ejecutamos la siguiente acción:

chkconfig --level 345 portmap off

RESTORECOND Se usa monitorizar y restaurar file context para SELinux. Puede deshabilitarlo con: chkconfig --level 345 restorecond off

RPCGSSD / RPCIDMAPD Servicios utilizados por NFS, si usted no utiliza este protocolo, debe deshabilitarlo. Para desactivar este servicio ejecutamos la siguiente acción:

chkconfig –level 345 rpcgssd off

chkconfig –level 345 rpcidmapd off 11

WANROUTER Es el driver para las tarjetas Sangoma, si no utiliza una en el servidor de comunicaciones es recomendable desactivarlo. Para desactivar este servicio ejecutamos la siguiente acción:

Chkconfig –level 345 wanrouter off

XINETD A través de xinetd se puede hacer uso de funciones especiales, tales como el tftp. En el caso de ser vulnerado puede dar un riesgo a nivel seguridad. Si no va a utilizar el servicio de tftp puede deshabilitarlo ejecutando la siguiente acción:

chkconfig –level 345 xinetd off

4.- CREAR UN USUARIO Y ASIGNARLO AL GRUPO WHEEL

Para ello hay que editar el archivo /etc/pam.d/su en el cual se encuentran las condiciones de autenticación para emplear el comando :

#vim /etc/pam.d/su

#%PAM-1.0

Auth sufficient pam_rootok.so

Uncomment the following line to implicitly trust users in the "wheel" group.

#auth sufficient pam_wheel.so trust use_uid

Uncomment the following line to require a user to be in the "wheel" group.

#auth required pam_wheel.so use_uid

auth include system-auth

account sufficient pam_succeed_if.so uid = 0 use_uid quiet

account include system-auth

password include system-auth 13

session include system-auth

session optional pam_xauth.so

Se debe descomentar la siguiente línea:

auth required pam_wheel.so use_uid

Tal como dice el comentario que precede esa línea al descomentar la misma se requiere ser del grupo wheel para poder utilizar el comando “su”

Si quita el comentario a la siguiente línea implica confianza en los usuarios del grupo Wheel:

auth sufficient pam_wheel.so trust use_uid

Le brindara a cualquier usuario del grupo Wheel la posibilidad de cambiar a superusuario sin la necesidad de introducir password. Por supuesto que esta opción es inaceptable desde el punto de vista de la seguridad del sistema. Por lo tanto únicamente es necesario descomentar la línea:

auth required pam_wheel.so use_uid

Para archivo quede de la siguiente manera:

#cat /etc/pam.d/su

#%PAM-1.0

auth sufficient pam_rootok.so

Uncomment the following line to implicitly trust users in the "wheel" group.

#auth sufficient pam_wheel.so trust use_uid

Uncomment the following line to require a user to be in the "wheel" group.

auth required pam_wheel.so use_uid

auth include system-auth

account sufficient pam_succeed_if.so uid = 0 use_uid quiet

account include system-auth

password include system-auth

session include system-auth

session optional pam_xauth.so

Ahora simplemente se debe crear un usuario y asignarlo al grupo Wheel

adduser-G wheel -m -s /bin/bash DianitaY

passwdDianitaY

De esta manera el usuario DianitaY podrá utilizar el comando “su” para convertirse en superusuario.

Sin embargo cualquier otro usuario no podrá hacerlo.

5.- ACTIVACIÓN DE FIREWALL ELASTIX

A NIVEL DE COMANDOS

Se borran las reglas anteriores

#iptables –F

#iptables –F –t nat

Aceptar todo a local loop

#iptables -A INPUT -i lo -j ACCEPT

Aceptar la red interna

#iptables -A INPUT -s 192.168.0.0/24 -d 0/0 -j ACCEPT

Aceptar el trafico SIP

#iptables -A INPUT -p udp -m udp --dport 5060 -j ACCEPT

#iptables -A INPUT -p tcp -m tcp --dport 5060 -j ACCEPT

#iptables -A INPUT -p tcp -m tcp --dport 5061 -j ACCEPT

Se agrega el seguimiento de conexiones sólo para una conexión existente y una

relacionada tanto para la cadena input y output

#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Estas líneas permitirán el trafico RTP.

#iptables -A INPUT –p udp –m udp –dport 10000:20000 –j ACCEPT

Aceptar el tráfico IAX2.

iptables -A INPUT -p udp -m udp -i eth0 --dport 4569 -j ACCEPT

Aceptar el tráfico del servidor de correo y POP/IMAP:

iptables -A INPUT -p tcp -i eth0 --dport 25 -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport 110 -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport 143 -j ACCEPT

Aceptar tráfico Web (HTTPS) para poder visitar la interface administrativa de Elastix:

iptables -A INPUT -p tcp -i eth0 --dport 443 -j ACCEPT

Finalmente denegando el acceso a todo lo demás:

#iptables -A INPUT -p all -i eth0 -j DROP

Para verificar si las reglas se aplicaron correctamente utilizar el comando:

#iptables –L –n –v

Luego para guardar las reglas de iptables

#service iptables save

A NIVEL DE INTERFAZ GRÁFICA

Se configura para que solo accedan a los servicios https, http y ssh desde la ip 192.168.1.6

Para más detalle [14].

6.- CONFIGURACIÓN DE FAIL2BAN

Hay que configurar Fail2Ban para que analice los logs que deseamos y bloquee IP's, enviando notificaciones vía e-mail. Para ello se modificara el archivo jail.conf que encontramos en /etc/fail2ban

cd /etc/fail2ban

vimjail.conf

Lo primero a modificar es el valor bantime, este valor determina el tiempo en segundos que quedará bloqueada la IP del atacante, por defecto el valor viene en 600 segundos.

Después buscar el valor maxretry que serán el número de veces que una IP puede tener una autenticación fallida antes de ser bloqueada.

fail2ban y SSH

Para que busque intentos fallidos de logueo por SSH modificar el archivo hasta que sea similar a las siguientes líneas:

[ssh-iptables] # Configuración de fail2ban para el puerto ssh

enabled = true

filter = sshd

action = iptables[name=SSH, port=37037, protocol=tcp] 25

sendmail-whois[name=SSH, dest=dyjaramil@gmail.com,

sender= soporte@mielastix] #fail2ban@localhost]

logpath = /var/log/secure # Este es el log que analizará fail2ban

maxretry = 3 # cualquier IP que tenga tres o más intentos erroneos se bloqueara.

bantime = 86400 # Tiempo de baneo de 24 horas expresado en segundos

Ahora se debe configurar para que fail2ban lea los registros de Asterisk

#cd /etc/fail2ban/filter.d

Crear el archivo asterisk.conf

#vimasterisk.conf

[INCLUDES]

[Definition]

failregex = NOTICE.* .*: Registration from '.*' failed for '' - Wrong password

NOTICE.* .*: Registration from '.*' failed for '' - No matching peer found

NOTICE.* .*: Registration from '.*' failed for '' - Username/auth name mismatch

NOTICE.* failed to authenticate as '.*'$

NOTICE.* .*: No registration for peer '.*' (from)

NOTICE.* .*: Host failed MD5 authentication for (*.) '*.'

NOTICE.* .*: Registration from '.*' failed for '' – Device does not match ACL

NOTICE.* .*: Failed to authenticate user .*@.*

ignoreregex =

Con esto le indica a fail2ban que tiene que controlar eventuales accesos indeseados en el archivo de registro de Asterisk.

Luego hay que modificar el archivo de configuración de fail2ban

cd /etc/fail2ban

vimjail.conf

Añadir al final del archivo de texto las siguientes líneas

[asterisk-iptables]

enabled = true

filter = asterisk

action = iptables-allports[name=ASTERISK, protocol=all] sendmail-whois[name=ASTERISK, dest=dyjaramil@gmail.com, sender=soporte@mielastix]

logpath = /var/log/asterisk/full

maxretry = 3

bantime = 86400

Para que funcione este nuevo jail hay que chequear la configuración de los archivos de registro de Asterisk:

#vim /etc/asterisk/logger.conf

Agregar las siguientes líneas al inicio.

[general]

dateformat=%F %T

Recargar el modulo de asterisk

#asterisk –rx “module reload”

Fail2ban y apache2

Otro servicio que se puede monitorear con fail2ban son los intentos fallidos de logeo en Apache2, para ello solo hay que cambiar algunos parámetros en el archivo jail.conf

enabled = true

port = http,https

filter = apache-auth

logpath = /var/log/httpd/ssl_error_log.log

#logpath = /var/log/apache*/*error.log 27

maxretry = 6

Reiniciar el servicio de fail2ban para que tome en cuenta las modificaciones realizadas

service fail2ban restart

Starting fail2ban: [OK]

Para lograr que fail2ban al inicio del sistema, ejecutar:

#chkconfig fail2ban on

Es una herramienta muy flexible que permitirá realizar los filtros que crea necesario.

7.- ASEGURAR HTTPS

#vim /etc/httpd/conf.d/elastix.conf

Apache-level configuration for Elastix administration interface

Timeout 300

Default apache configuration specifies greater limits than these

#MaxClients 150

#MaxRequestsPerChild 1000

Default apache User and Group directives MUST be commented out

in order for these to take effect. 22

User asterisk

Group asterisk

<Directory “/var/www/html”>

Redirect administration interface to https

RewriteEngine On

RewriteCond %{HTTPS} off

RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}

AuthType Basic

AuthName "ZONA RESTRINGIDA. THIS IS SPARTA"

AuthUserFile /usr/local/apache/wwwpasswd

RequireuserelastixDianitaY

</Directory >

El siguiente paso es generar el password con el comando htpasswd:

mkdir /usr/local/apache

#htpasswd –c /usr/local/apache/wwwpasswdDianitaY

Luego solicitara ingresar un password, finalizados estos pasos es necesario reiniciar apache para que tome los cambios

#servicehttpdrestart

8.- CONFIGURACIÓN PARA EVITAR ESCANEOS Y ENUMERACIÓN

Para no mostrar el tipo de central, se configura en el archivo sip_general_custom.conf lo siguiente:

useragent=Another

sdpsession=Another

sdpowner=WonderWoman

Para evitar enumeración de extensiones se configura en el archivo sip_general_custom.conf lo siguiente:

alwaysauthreject=yes

Para evitar escaneos y enumeración, e configura lo siguiente en iptables:

iptables -N SIPDOS

iptables -A INPUT -i eth0 -p udp -m udp –dport 5060 -m string –string “sundayddr” –algo bm –to 65535 -m comment –comment “deny sundayddr” -j SIPDOS

iptables -A INPUT -i eth0 -p udp -m udp –dport 5060 -m string –string “sipsak” –algo bm –to 65535 -m comment –comment “deny sipsak” -j SIPDOS

iptables -A INPUT -i eth0 -p udp -m udp –dport 5060 -m string –string “sipvicious” –algo bm –to 65535 -m comment –comment “deny sipvicious” -j SIPDOS

iptables -A INPUT -i eth0 -p udp -m udp –dport 5060 -m string –string “friendly-scanner” –algo bm –to 65535 -m comment –comment “deny friendly-scanner” -j SIPDOS

iptables -A INPUT -i eth0 -p udp -m udp –dport 5060 -m string –string “iWar” –algo bm –to 65535 -m comment –comment “deny iWar” -j SIPDOS

iptables -A INPUT -i eth0 -p udp -m udp –dport 5060 -m string –string “sip-scan” –algo bm –to 65535 -m comment –comment “deny sip-scan” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5060 -m string –string “sundayddr” –algo bm –to 65535 -m comment –comment “deny sundayddr” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5060 -m string –string “sipsak” –algo bm –to 65535 -m comment –comment “deny sipsak” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5060 -m string –string “sipvicious” –algo bm –to 65535 -m comment –comment “deny sipvicious” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5060 -m string –string “friendly-scanner” –algo bm –to 65535 -m comment –comment “deny friendly-scanner” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5060 -m string –string “iWar” –algo bm –to 65535 -m comment –comment “deny iWar” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5060 -m string –string “sip-scan” –algo bm –to 65535 -m comment –comment “deny sip-scan” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5061 -m string –string “sundayddr” –algo bm –to 65535 -m comment –comment “deny sundayddr” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5061 -m string –string “sipsak” –algo bm –to 65535 -m comment –comment “deny sipsak” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5061 -m string –string “sipvicious” –algo bm –to 65535 -m comment –comment “deny sipvicious” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5061 -m string –string “friendly-scanner” –algo bm –to 65535 -m comment –comment “deny friendly-scanner” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5061 -m string –string “iWar” –algo bm –to 65535 -m comment –comment “deny iWar” -j SIPDOS

iptables -A INPUT -i eth0 -p tcp -m tcp –dport 5061 -m string –string “sip-scan” –algo bm –to 65535 -m comment –comment “deny sip-scan” -j SIPDOS

iptables -A SIPDOS -j LOG –log-prefix “firewall-sipdos: ” –log-level 6

iptables -A SIPDOS -j DROP