ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELETRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ELECTRÓNICO EN REDES Y COMUNICACIÓN DE DATOS

AUTOR: SOTOMAYOR POZO, JULIO CÉSAR

TEMA: ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD EN CENTRALES VoIP ELASTIX A TRAVÉS DE HACKING ÉTICO.

DIRECTOR: ING. ROMERO, CARLOS

CODIRECTOR: ING. SAENZ, FABIAN

SANGOLQUÍ, AGOSTO 2014

CERTIFICACIÓN

Certificamos que el siguiente proyecto de grado titulado: ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD EN CENTRALES VoIP ELASTIX A TRAVÉS DE HACKING ÉTICO., ha sido desarrollado en su totalidad por el señor JULIO CÉSAR SOTOMAYOR POZO, bajo nuestra dirección

Atentamente,

_____	_____
Ing. Carlos Romero	Ing. Fabián Sáenz
DIRECTOR	CODIRECTOR

DECLARACIÓN DE RESPONSABILIDAD

JULIO CÉSAR SOTOMAYOR POZO

DECLARO QUE:

El proyecto denominado "**ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD EN CENTRALES VoIP ELASTIX A TRAVÉS DE HACKING ÉTICO.**", ha sido desarrollado en base a una investigación exhaustiva, respetando los derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 15 de agosto de 2014

_____

Julio César Sotomayor Pozo

AUTORIZACIÓN

JULIO CÉSAR SOTOMAYOR POZO

Autorizo a la Universidad de las Fuerzas Armadas “ESPE” la publicación, en la biblioteca virtual de la Institución del trabajo “ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD EN CENTRALES VoIP ELASTIX A TRAVÉS DE HACKING ÉTICO.”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 15 de agosto de 2014

_____

Julio César Sotomayor Pozo

DEDICATORIA

El presente proyecto de grado se lo dedico a Dios que ha sido mi guía y protector a lo largo de mi vida, a mis padres que han sido un ejemplo de vida y mis hermanas que con sus sabios consejos me han guiado por el camino correcto.

Julio César Sotomayor Pozo

AGRADECIMIENTOS

Agradezco a Dios y la Virgencita Dolorosa por cuidarme, bendecirme y protegerme en cada instancia de mi vida.

A mis padres por luchar incansablemente por mi bienestar, aconsejarme y soportar mis momentos de ira.

A mis hermanas, por ser un ejemplo a seguir, demostrándome con sus experiencias de vida que solo luchando con perseverancia se alcanzan nuestras metas.

A mi abuelitos, que ahora, todos juntos desde el cielo guían mis pasos.

A mi novia que desde hace 5 años comparte alegrías y tristezas junto a mí y ha sido mi soporte en todo momento.

A mi gran amigo Daniel Guevara, quien fue pilar fundamental en el desarrollo de este proyecto.

A mi director y codirector, Ing. Carlos Romero e Ing. Fabián Saenz por su excelente labor como docentes.

A mis jefes y compañeros en AyalaConsulting, que me han permitido desarrollar este proyecto a la par con mi trabajo.

Y a todas aquellas personas que de una u otra forma han sido parte de mi vida.

Julio César Sotomayor Pozo

RESUMEN

Las comunicaciones a través de telefonía IP se han incrementado notablemente en los últimos años, cada día más empresas ven como solución con bajo costo la implementación de VoIP y específicamente la plataforma Elastix es actualmente una de las más usadas a nivel mundial. Es necesario entonces garantizar la seguridad que brinda ésta plataforma tanto a nivel de confidencialidad como de infraestructura y el hacking ético se presenta como una herramienta para poner a prueba la seguridad de éstas centrales telefónicas.

El presente proyecto de grado se ha desarrollado específicamente para buscar vulnerabilidades de las centrales Elastix y determinar las soluciones más eficientes a las mismas, para lo cual se procede a realizar pruebas de penetración basadas en hacking ético, que permitan determinar sus puntos débiles y fortalecer los mismos, comprobando después con las mismas herramientas si las vulnerabilidades aún persisten o fueron solucionadas.

PALABRAS CLAVE:

- **VOIP**
- **ELASTIX**
- **HACKING ÉTICO**
- **VULNERABILIDAD**
- **KALI LINUX**

ABSTRACT

Communications through IP telephony have significantly increased in the last few years. Every day more companies opt for the implementation of VoIP as a low cost solution and specifically Elastix is currently one of the most commonly used platforms worldwide. Therefore, it is necessary to guarantee the security offered by this platform in terms of both confidentiality and infrastructure, and ethical hacking is presented as a tool to test the security of IP PBX.

This thesis project has been specifically developed to search for vulnerabilities in the Elastix IP PBX and to establish the most efficient solutions to address such vulnerabilities. Penetration tests based on ethical hacking are therefore used to determine weaknesses and strengthen them, followed by subsequent tests using the same tools to verify whether such vulnerabilities still persist or were overcome.

ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD EN CENTRALES VoIP ELASTIX A TRAVÉS DE HACKING ÉTICO.

INDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

ADMINISTRADOR, sysop, root: Esla persona que se encarga del sistema. Sé suele denominar root y es la persona que tiene el poder absoluto sobre la máquina.

AGUJERO, bug, hole: Es un defecto en el software o hardware que como su nombre indica deja agujeros para los hackers

ASTERISK: Asterisk es un programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX).

BUGS y EXPLOITS: Los bugs son fallos en el software o en el hardware y que usan los hackers para entrar en sistemas y un exploit es un programa que aprovecha el agujero dejado por el bug...

BOMBA LOGICA: Código que ejecuta una particular manera de ataque cuando una determinada condición se produce. Por ejemplo una bomba lógica puede formatear el disco duro un día determinado, pero a diferencia de un virus.

BACKDOOR puerta trasera. Mecanismo que tiene o que se debe crear en un software para acceder de manera indebida.

BOXING: Uso de aparatos electrónicos o eléctricos (Boxes) para hacer phreaking. Esto no es hacking sino phreaking.

CABALLOS DE TROYA: Programa que se queda residente en un sistema y que ha sido desarrollado para obtener algún tipo de información

CLOACKER: Programa que borra los logs (huellas) en un sistema. También llamados zappers.

CRACKER: Esta palabra tiene dos acepciones, por un lado se denomina CRACKER a un HACKER que entra a un sistema con fines malvados aunque normalmente la palabra CRACKER se usa para denominar a la

gente que desprotege programas, los modifica para obtener determinados privilegios, etc.

CRACKEADOR DE PASSWORDS: Programa utilizado para sacar los password encriptados de los archivos de passwords.

CRACKING: Actividad destinada a la desprotección de programas de todo tipo que piden un numero serial o una clase de acceso. El cracking obviamente se usa también para descifrar claves para desencriptar datos.

CRASHING: Esta actividad es una variación del cracking; consiste en adulterar programas que originalmente son inofensivos agregándole códigos dañinos para destruir los datos almacenados en la computadora de sus enemigos.

DAEMON: Proceso en background en los sistemas Unix, es decir un proceso que esta ejecutándose en segundo plano.

ELASTIX: Elastix es una distribución libre de Servidor de Comunicaciones Unificadas que integra en un solo paquete

EXPLOIT Método concreto de usar un bug para entrar en un sistema.

FUERZA BRUTA (hackear por...) Es el procedimiento que usan tanto los crackeadores de password de UNIX que se basan en aprovechar diccionarios para comparar con los passwords del sistema para obtenerlos.

FAKE MAIL: Enviar correo falseando el remitente. Es muy útil en ingeniería social.

GUSANO: Termino famoso a partir de Robert Morris, Jr.Gusanos son programas que se reproducen ellos mismos copiándose una y otra vez de sistema a sistema y que usa recursos de los sistemas atacados.

IAX: Acrónimo de “Inter Asterisk Exchange”.

INGENIERIA SOCIAL: Obtención de información por medios ajenos a la informática.

ISP (Internet Services Provider): Proveedor de servicios internet.

KEY: Llave. Se puede traducir por clave de acceso a un software o sistema.

KERBEROS: Sistema de seguridad en el que los login y los passwords van encriptados.

LAMER: Un lamer es una persona que no tiene ninguna inquietud por todos estos temas de la seguridad sino que lo único que quiere es tener un login y un pass para entrar a un sistema y formatear el disco duro

LINUX: Sistema operativo de la familia UNIX y que es muy adecuado para tenerlo en la máquina de casa ya que no requiere demasiados recursos.

LOGIN: Para entrar en un sistema por telnet se necesita siempre un login (nombre) y un password (clave).

PASSWORD: Contraseña asociada a un login.

PIRATA: Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado.

PORT SCANNER: Programa que te indica que puertos de una maquina están abiertos.

ROUTER: Maquina de la red que se encarga de encauzar el flujo de paquetes.

SIP: (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet

SNIFFER: Es un programa que monitoriza los paquetes de datos que circulan por una red.

TCP/IP: Arquitectura de red con un conjunto de protocolos.

VIRUS: Es un programa que se reproduce a sí mismo y que muy posiblemente ataca a otros programas.

VoIP: Es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite comunicar voz sobre el protocolo IP

CAPÍTULO I: INTRODUCCIÓN

1.1. ANTECEDENTES

Debido al continuo avance de la tecnología, la telefonía análoga en inclusive la digital se ha visto desplazadas por la telefonía IP o VoIP.
Esto sucede básicamente por las ventajas que presenta VoIP ya que permite la unión de dos mundos históricamente separados, el de la transmisión de voz y el de la transmisión de datos. Entonces, VoIP puede transformar una conexión standard a internet en una plataforma para realizar llamadas gratuitas por internet.

En el pasado, las conversaciones mediante VoIP solían ser de baja calidad, esto se vio superado por la tecnología actual y la proliferación de conexiones de banda ancha.
Se sabe que va a llevar algún tiempo pero es seguro que en un futuro cercano desaparecerán por completo las líneas de teléfono convencionales que utilizamos en nuestra vida cotidiana, el avance tecnológico indica que estas serán muy probablemente reemplazadas por la telefonía IP.

En este nuevo enfoque, donde antes teníamos dos redes completamente separadas, ahora tenemos dos redes unidas que comparten los recursos tanto físicos como lógicos y es por esto que aparecen dudas acerca de si la telefonía seguirá teniendo el grado de seguridad que posee en la actualidad con las soluciones tradicionales, ya que, con el paso de los años, la telefonía tradicional ha alcanzado niveles de seguridad aceptables.

Por esta razón se han generado temores respecto de la seguridad cuando se habla de implementar soluciones de telefonía IP. Si bien los proveedores de las soluciones han declarado que éstas involucran cada vez más a la seguridad como un factor clave en su diseño, los riesgos aún existen.

¿Cuáles son estos riesgos?

Al utilizar soluciones basadas en Telefonía IP, cobra mucha más fuerza la frase que compara la seguridad con una cadena: "La cadena se romperá por el eslabón más débil". Y esto es lo mismo que decir que el nivel de seguridad de toda la solución será tan fuerte como el más débil de sus componentes.

En una solución de telefonía IP existen diversos componentes que podrán ser el objetivo de ataques. Si bien cada solución de diferentes proveedores tiene sus componentes específicos podemos citar en general los siguientes:

- *Emisor y Receptor, es decir, los participantes de la comunicación y sus respectivas identidades*
- *El mensaje que es transmitido durante la conversación*
- *Los equipos que componen la solución de telefonía IP y los servicios que éstos brindan*

De este modo, un ataque a la seguridad de los mismos nos dará como resultado diversos riesgos. Los riesgos no son nuevos a causa del uso de soluciones de Telefonía IP, sino que se ven potenciados por el mismo. Podemos agrupar los riesgos en:

- *Riesgo de robo de identidad.*
- *Riesgo de escucha de conversaciones.*
- *Riesgo de robo de servicio o fraude*
- *Riesgo de disponibilidad de la solución.*

Tomando esto en cuenta la implementación de soluciones de Telefonía IP supone nuevos riesgos aplicados a los servicios de telefonía. El costo de asegurar más la Telefonía IP, tiene que estar determinado de acuerdo al costo de las pérdidas al negocio que ocasionaría cualquiera de los ataques que ésta pudiera sufrir.

Existen varias plataformas de telefonía IP, en nuestro país la más utilizada es Elastix, la cual es un software libre licenciado en Ecuador bajo GPL versión 2. Esta plataforma es muy amigable y ha ganado muchos usuarios en los últimos años, sin embargo como toda plataforma tecnológica existen vulnerabilidades en su seguridad, las cuales muchas veces no son tomadas en cuenta y pueden desencadenar en problemas graves para los usuarios o peor aún para toda una empresa.

1.2. JUSTIFICACIÓN E IMPORTANCIA

La seguridad en las plataformas que manejamos dentro de nuestras empresas es fundamental y muchas veces no se le da la importancia adecuada, por ello surge la necesidad de prevenir posibles ataques, encontrando las vulnerabilidades que posee nuestra plataforma Elastix y el mejor método para realizarlo se nos presenta a través del Hacking Ético, ya que a través de él es posible detectar el nivel de seguridad interno y externo de las plataformas, para así determinar el grado de acceso que tendría un atacante con intenciones maliciosas y de esta manera poder prevenirlo.

La importancia del desarrollo de este proceso viene dada por la capacidad que será adquirida para mejorarla seguridad de nuestra plataforma, evitando el fácil acceso a nuestra información y protegiendo la integridad de nuestras comunicaciones años atrás un mensaje escrito en un papel dio por terminadas guerras, hoy una llamada segura y a tiempo podría prevenirlas.

1.3. ALCANCE

Este proyecto llevará a cabo un estudio de vulnerabilidades de centrales de VoIP Elastix a través de un proceso de Hacking Ético, para

lo cual se estudiara los métodos de ataque existentes, las herramientas de hardware y software necesarias.

Para la comprobación de dichas vulnerabilidades se implementara tanto la central Elastix como el software para el Hacking Ético en ambientes virtuales y se utilizara la metodología OSSTMM (Open Source Testing Metdology Manual) de la OWASP (The Open Web Application Security Project) [6]

Después de terminado el proceso de ataque se enlistaran las vulnerabilidades encontradas y se plantearan posibles métodos de protección para las mismas, siendo estas soluciones de interés para todos los distribuidores y usuarios de Elastix.

1.4. OBJETIVOS

1.4.1. General

Analizar las vulnerabilidades en seguridad que poseen las centrales de VoIP Elastix e implementar soluciones adecuadas para la prevención de posibles ataques.

1.4.2. Específicos

a) Introducir el hacking ético y la terminología esencial.
b) Entender las diferentes fases seguidas por un hacker.
c) Encontrar vulnerabilidades de la central Elastix a través de Hacking Ético.
d) Implementar soluciones a las vulnerabilidades encontradas.
e) Determinar mediante los resultados obtenidos de las pruebas realizadas las conclusiones y recomendaciones para futuros trabajos de investigación.

1.5. INTRODUCCIÓN A VOIP

1.5.1. ¿Qué es VoIP?

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, (VoIP por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local (LAN).

1.5.2. Elementos de VoIP

El cliente

El cliente establece y origina las llamadas voz, esta información se recibe a través del micrófono del usuario (entrada de información) se codifica, se empaqueta y, de la misma forma, esta información se decodifica y reproduce a través de los altavoces o audífonos (salida de la información).

Un Cliente puede ser un usuario de Skype o un usuario de alguna empresa que venda sus servicios de telefonía sobre IP a través de equipos como ATAs (Adaptadores de teléfonos analógicos) o teléfonos IP o Softphones que es un software que permite realizar llamadas a través de una computadora conectada a Internet.

Los servidores

Los servidores se encargan de manejar operaciones de base de datos, realizado en un tiempo real como en uno fuera de él. Entre estas operaciones se tienen la contabilidad, la recolección, el enrutamiento, la administración y control del servicio, el registro de los usuarios.

Usualmente en los servidores se instala software denominados Switches o IP-PBX (Conmutadores IP), ejemplos de switches pueden ser "Voipswitch", "Mera", "Nextone" entre otros, un IP-PBX es Asterisk uno de los más usados y de código abierto.

Los gateways

Los gateways brindan un puente de comunicación entre todos los usuarios, su función principal es la de proveer interfaces con la telefonía tradicional adecuada, la cual funcionara como una plataforma para los usuarios (clientes) virtuales.

Los Gateways se utilizan para "Terminar" la llamada, es decir el cliente Origina la llamada y el Gateway Termina la llamada, eso es cuando un cliente llama a un teléfono fijo o celular, debe existir la parte que hace posible que esa llamada que viene por Internet logre conectarse con un cliente de una empresa telefónica fija o celular.

CAPITULO II: ANÁLISIS DE LA ESTRUCTURA DE ELASTIX

2.1. ¿QUÉ ES ELASTIX?

Elastix es una aplicación software para crear sistemas de Telefonía IP, que integra las mejores herramientas disponibles para PBXs basados en Asterisk en una interfaz simple y fácil de usar. Además añade su propio conjunto de utilidades y permite la creación de módulos de terceros para hacer de este el mejor paquete de software disponible para la telefonía de código abierto.

La meta de Elastix son la confiabilidad, modularidad y fácil uso. Estas características añadidas a la robustez para reportar hacen de él, la mejor opción para implementar un PBX basado en Asterisk.

2.2. PROTOCOLOS DE TRABAJO.

Hay muchos protocolos involucrados en la transmisión de voz sobre IP. Ya de por sí hay protocolos de red involucrados como el propio protocolo IP y otros protocolos de transporte como TCP o UDP. Encima de ellos se colocan los protocolos de señalización de voz y como si esto fuera poco existen además muchas opciones de protocolos de señalización disponibles lo que puede hacer que todo suene un poco confuso al principio.

Para simplificar las cosas podríamos clasificar a los protocolos utilizados en la VoIP en tres grupos.

- Protocolos de señalización
- Protocolos de transporte de voz

Protocolos de señalización

Los protocolos de señalización en VoIP cumplen funciones similares a sus homólogos en la telefonía tradicional, es decir tareas de establecimiento de sesión, control del progreso de la llamada, entre otras.

Se encuentran en la capa 5 del modelo OSI, es decir en la capa de Sesión

Existen algunos protocolos de señalización, que han sido desarrollados por diferentes fabricantes u organismos como la ITU o el IETF, y que se encuentran soportados por Elastix. Algunos son:

- SIP
- IAX
- H.323
- MGCP
- SCCP

Protocolos de transporte de voz

No se debe confundir aquí con protocolos de transporte de bajo nivel como TCP y UDP. Nos referimos aquí al protocolo que transporta la voz propiamente dicha o lo que comúnmente se denomina carga útil. Este protocolo se llama RTP (Real-time Transport Protocol) y función es simple: transportar la voz con el menor retraso posible.

Este protocolo entra a funcionar una vez que el protocolo de señalización ha establecido la llamada entre los participantes.

2.3. PUERTOS COMUNES DE FUNCIONAMIENTO.

Una de las prestaciones que nos da la telefonía IP de manera nativa y que es casi imposible lograrlo en los sistemas telefónicos tradicionales sin hacer uso de gateway, es la de permitir instalar extensiones en sitios remotos localizadas fuera del recinto donde se encuentra la PBX-IP, “el único requisito” es que haya un canal de comunicación desde y hacia la red IP donde se encuentra instalado el servidor Elastix , así como desde y hacia las diferentes localidades donde estén instalados los teléfonos IP, para que se puedan comunicar entre ellos.

Cuando se instalan extensiones fuera de la red IP a la que pertenece el servidor Elastix, se presentan una serie de problemas que se complican aún más cuando existen router y firewall de por medio y más

aún si las extensiones se encuentran instaladas en diferentes localidades con diferentes redes IP o desde el Internet.

En los sistemas telefónicos Asterisk-Elastix intervienen una serie de protocolos para el establecimiento de una llamada entre dos o más teléfonos IP, de manera nativa se utilizan los protocolos SIP e IAX2. Estos a su vez viajan encapsulados en paquetes TCP/UDP sobre redes IP.

Puertos UDP/TCP para el protocolo SIP.

SIP se complementa con SDP (Session Description Protocol) y RTP (Real Time Protocol), SDP para el envío de los detalles del contenido multimedia de la sesión, como por ejemplo direcciones IP, puertos, y códec que se usaran durante la comunicación, y RTP para la transmisión de los datos, ya sean voz, video u otros multimedia, entre los participantes de la comunicación, que previamente se estableció por SIP.

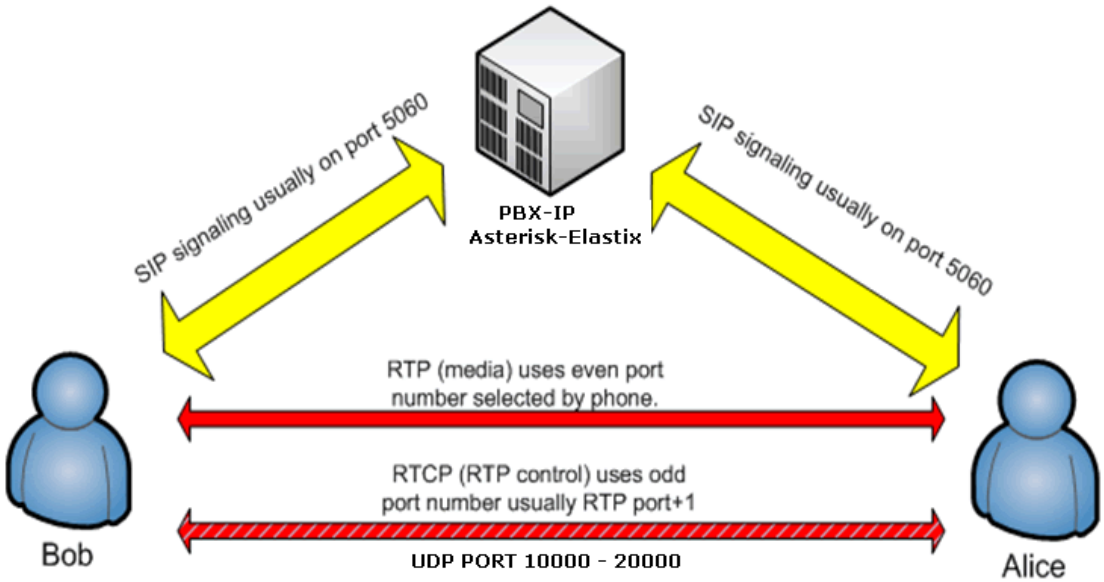


FIGURA 1: PUERTOS TCP/UDP UTILIZADOS POR SIP EN ELASTIX

En el momento que se realiza una llamada entre dispositivos o teléfonos IP que utilizan el protocolo SIP, se hace siguiendo el siguiente proceso:

1.- El teléfono IP del llamante, solicita al servidor Elastix que establezca una conexión con el Teléfono IP que tiene el número de la extensión destino, esto se hace por medio del protocolo SDP haciendo uso del puerto UDP 5060 en algunos casos también se utiliza el puerto TCP 5060.

2.- El servidor Elastix contacta con el teléfono IP destino utilizando el mismo protocolo SDP a través de los mismos puertos UDP/TCP 5060.

3.- El servidor Elastix establece la comunicación entre los 2 teléfonos IP, comunicando el dispositivo de la extensión origen con la extensión destino. Una vez queda establecida la comunicación (sesión) el servidor Elastix ya no interviene en ella. Todo este proceso se realiza por medio de paquetes SIP-SDP a través del puerto TCP-UDP 5060.

4.- Los 2 teléfonos IP inician la transferencia de la voz de manera bidireccional, haciendo una conexión punto a punto (peer to peer), por medio del protocolo RTP abriendo un puerto aleatorio UDP que esta entre 10000 a 20000. Para que la transferencia de la voz se realice en ambos sentidos, debe existir un puerto UDP abierto en ambos lados del canal de comunicación establecido, si el puerto UDP únicamente está abierto en un solo lado o en una sola dirección del canal IP, la voz viajara en un solo sentido, lo que provoca que solo se escuche únicamente a un lado o que no se escuche nada en ambos lados.

5.- Cuando la llamada se finaliza se vuelve a contactar al servidor Elastix, siguiendo un proceso similar descrito en el paso 1.

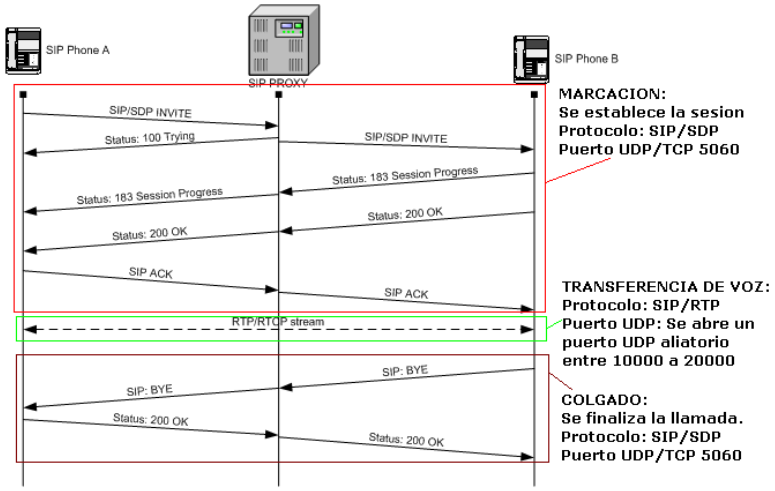


FIGURA 2: LLAMADA SIP Y PUERTOS UDP/TCP QUE SE UTILIZAN.

Es importante tener en mente que la comunicación es bidireccional por lo tanto se deben abrir los puertos UDP 10000 a 20000 para trafico entrante y saliente, así como el puerto UDP/TCP 5060, si hay un firewall de por medio en cada localidad, se deben configurar para permitir este tráfico en cada una de las redes IP donde existan teléfonos IP, de lo contrario no van a poder comunicarse.

Puertos UDP/TCP para el protocolo IAX2

IAX2 utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales (terminales VoIP) para señalización y datos. El tráfico de voz es transmitido in-band, lo que hace a IAX2 un protocolo casi transparente a los cortafuegos (Firewall) y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP out-of-band para entregar la información.

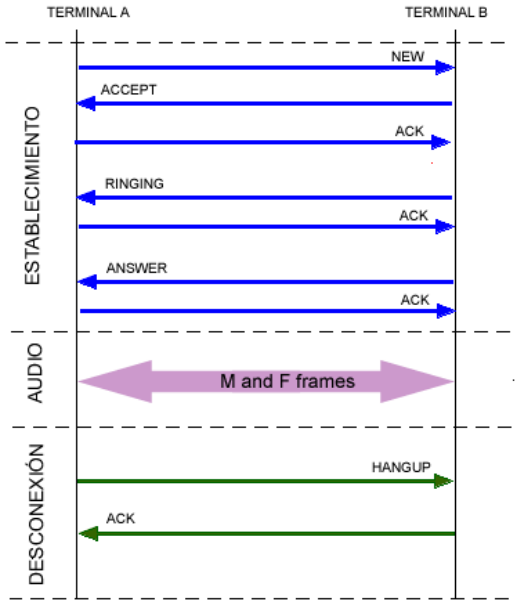


FIGURA 3: PUERTOS UDP/TCP PARA EL PROTOCOLO IAX2

IAX2 soporta Trunking, donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional. Esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado.

La estructura básica de IAX2 se fundamenta en la multiplexación de la señalización y del flujo de datos sobre un simple puerto UDP entre dos sistemas. IAX2 es un protocolo binario y está diseñado y organizado de manera que reduce la carga en flujos de datos de voz. El ancho de banda para algunas aplicaciones se sacrifica en favor del ancho de banda para VoIP.

Para evitar los problemas de NAT el protocolo IAX o IAX2 usa como protocolo de transporte UDP, normalmente sobre el puerto 4569, (el IAX1 usaba el puerto 5036), y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP) y por tanto lo hace

menos proclive a problemas de NAT y le permite pasar los routers y firewalls de manera más sencilla.

2.4. VISIÓN A NIVEL DE ESTRUCTURA DE SOFTWARE.

Sistema de gestión de PBX Asterisk – Free PBX

FreePBX es una interfaz web de usuario que facilita la interoperabilidad del usuario con el sistema VoIP Asterisk. Abstrae en ciertas ocasiones de tareas de cierta complejidad y por tanto resulta muy útil para usuarios o administradores que no estén muy familiarizados con Asterisk. Corre bajo licencia GPL.

FreePBX Asterisk VoipSe estructura se divide modularmente y dispone de las siguientes funcionalidades del mundo VoIP. Cabe destacar:

- Módulo de lenguajes para la Internacionalización del sistema.
- Módulo de colas de llamadas.
- Condiciones de tiempo.
- Grupos de ringado.
- Colas de llamadas.
- Enrutamiento entrante.
- Reglas de enrutamiento saliente. Soporte SIP, IAX, DAHDI, ZAPTEL.
- Lista Negra.
- Módulo de locuciones.
- Módulo de Parking.
- Buzones de voz VoIP.
- FOP Flash Operator Panel.
- CDR Call Detail Records.

- IVR: Interactive Voice Response

Servicio de mensajería instantánea – Openfire

Openfire (anteriormente llamado Wildfire y Jive Messenger) es un sistema de mensajeria instantánea GPL y hecho en java y utiliza el protocolo XMPP con el podrás tener tu propio servidor de mensajería puedes administrar a tus usuarios, compartir archivos, auditar mensajes, mensajes offline, mensajes broadcast, grupos, etc y además contiene plugins gratuitos con diferentes funciones extras.

Panel Web de Administración de Openfire

La administración del servidor se hace a través de una interfaz web, que corre por defecto en el puerto 9090 (HTTP) y 9091 (HTTPS). Los administradores pueden conectarse desde cualquier lugar y editar la configuración del servidor, agregar y borrar usuarios, crear cuartos de conferencia permanentes, etc.

Características
Openfire implementa las siguientes características:

- Panel de administración web
- Interfaz para agregar plugins
- SSL/TLS
- Amigable
- Adaptable según las necesidades
- Conferencias
- Interacción con MSN, Google Talk, Yahoo messenger, AIM, ICQ, Jingle
- Estadísticas del Servidor, mensajes, paquetes, etc.
- Cluster con múltiples servidores

- Transferencia de Archivos
- Compresión de datos
- Tarjetas personales con Avatar
- Mensajes offline
- Favoritos
- Autenticación vía Certificados, Kerbeos, LDAP, PAM y Radius
- Almacenamiento en Active Directory, LDAP, MS SQL, MySQL, Oracle y PostgreSQL
- SASL: ANONYMOUS, DIGEST-MD5 y Plain

Servidor WEB – Apache

El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que Behelendorf quería que tuviese la connotación de algo que es firme y enérgico pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de EEUU, y en esos momentos la preocupación de su grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de internet. Además Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA.

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años. (Estadísticas históricas y de uso diario proporcionadas por Netcraft).

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

Sistema de CRM – Vtiger

Es una aplicación CRM de código abierto bifurcada con la intención de hacer una herramienta con una funcionalidad similar a SugarCRM y Salesforce.com, pero de código abierto. En su versión gratuita ofrece una herramienta de informes, un portal para clientes y un plugin para Outlook, opciones que se hallan en las versiones de pago de las otras aplicaciones.

Características
Las principales características incluidas en vtiger CRM son:

- Gestión automatizada de ventas (entradas de producto personalizables, gestión del inventario y proveedores, citaciones, facturaciones y sistema de seguimiento de incidentes.

- Servicio de ayuda al cliente y funciones del servicio, incluyendo un portal de autoservicio para el cliente.
- Automatización del mercado (estudio de clientes potenciales, apoyo de campañas y bases de conocimiento).
- Gestión del inventario.
- Análisis e informes.

También incluye características de interacción con el usuario como:

- Integración con sistemas de correo electrónico corporativo, mediante plugins o extensiones, para Microsoft Outlook y Mozilla Thunderbird.
- Soporte para el sistema telefónico Asterisk PBX.
- Calendario electrónico.
- Función de Nube de etiquetas.
- Suscripción a canales RSS.
- Generación de documentos PDF mediante la librería TCPDF.

2.5. TOPOLOGÍAS DE RED USADAS.

Las plataformas elastix se presentan principalmente con 2 tipos de topologías:

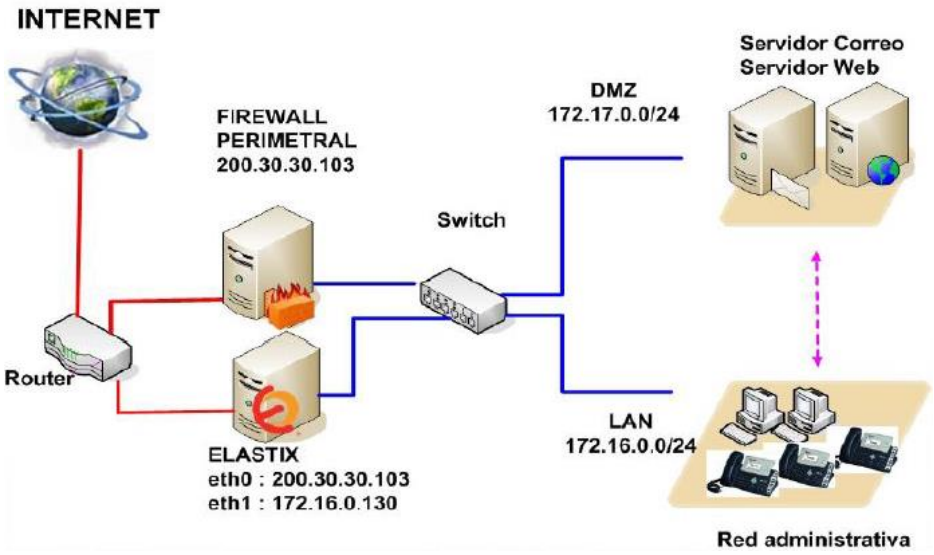


FIGURA 4: ELASTIX CON IP PÚBLICA + ESTÁTICA

En este primer caso la topología se muestra con la central IP saliendo a través de un router hacia el internet, en este caso el router asigna una dirección IP pública a una interfaz de red de la central mientras que otra interfaz es la que se comunica con la red interna (LAN), de este mismo tipo de topología pueden existir variaciones, pero siempre dejando a una interfaz de la central con una IP pública.

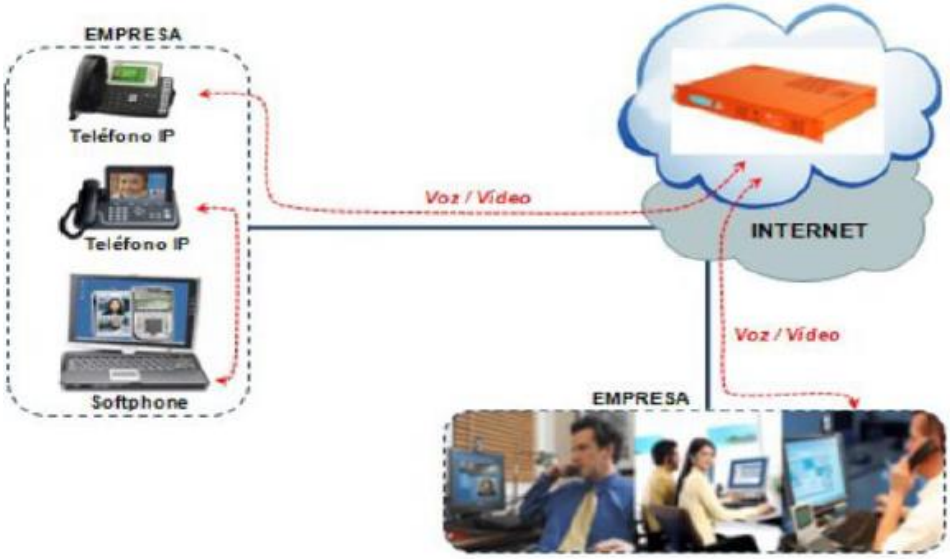


FIGURA 5: ELASTIX EN LA NUBE

En este segundo caso no existe una infraestructura como tal para la central, ésta reposa en un servidor virtual alojado en la nube de internet y tanto las personas de la red local como las exteriores acceden a ella mediante una dirección pública.

En ambos casos podemos notar que la central Elastix posee una IP pública, como veremos más adelante este es el punto de arranque donde empiezan las vulnerabilidades.

2.6. PARÁMETROS DE SEGURIDAD OFRECIDAS POR LA PLATAFORMA.

La seguridad de cualquier sistema informático es una responsabilidad del administrador de los sistemas, es una de las primeras tareas que se tienen que ejecutar, sin embargo casi siempre o no se hacen, o se dejan hasta el final en el mejor de los casos. Es muy común que esto se deje en un segundo plano, no dándole la importancia debida, hasta que ya es demasiado tarde y los sistemas se han visto comprometidos, para el caso de una PBX-IP con conexión a Internet este error puede salir muy caro.

Elastix a partir de la versión 2.0.4, incorpora un módulo de seguridad, basado en el Firewall de Linux IPTABLES, que sin bien es cierto es bastante básico, permite configurar lo necesario para minimizar el riesgo de accesos indebidos al servidor, así como restringir las redes IP que tendrán acceso a los servicios de telefonía que el servidor Elastix provee.

Está comprobado que el mayor porcentaje de intentos de accesos indebidos y ataques a los sistemas proviene de la Red Interna (LAN-WAN), la mayoría por usuarios que hacen escaneos de red e incluso ataques de fuerza bruta para averiguar las claves de los servidores.

Aunque el servidor Elastix no tenga extensiones remotas que se conecten vía Internet o vía una Wan, es importante restringir las redes IP desde donde se permitirán las conexiones, de igual forma se debe restringir los accesos a la consola Web y las sesiones SSH, ya que si un usuario no autorizado logra violar la seguridad, accediendo al servidor Elastix, por cualquiera de estos 2 métodos prácticamente tiene acceso total sobre él.

Restringir el acceso a la interface Web de administración, es lo mínimo que debemos de hacer para asegurar nuestro servidor Elastix, especialmente si estamos en una red con más de 20 usuarios activos, nunca se sabe quién estará por ahí haciendo travesuras en la red, si

dejamos el acceso a la interface Web abierta para que se pueda acceder desde cualquier punto de nuestra red, es como dejar la puerta abierta de nuestra casa, esta es la manera más básica y sencilla para ingresar al servidor Elastix. Por lo general como administrador del servidor Elastix ingresamos desde una sola computadora que a su vez tiene una única dirección IP, no es recomendable acceder desde cualquier punto ya que las credenciales de acceso (usuario/clave) a veces quedan registradas o guardadas en las computadoras desde donde ingresamos sin que nos demos cuenta de esto, aumentando la posibilidad de un acceso indebido, una buena práctica es habilitar el acceso a la interface Web desde una única dirección IP,

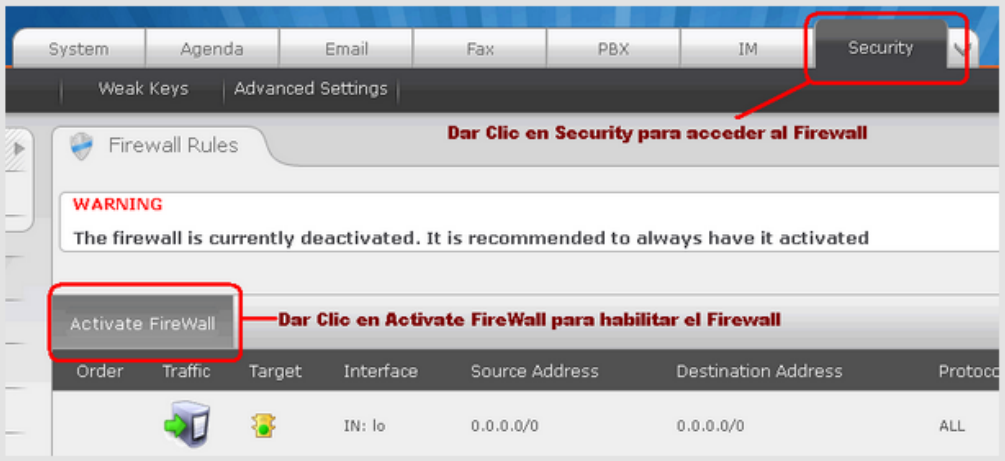


FIGURA 6: FIREWALL ELASTIX

CAPITULO III: HACKING ÉTICO ANÁLISIS DE VECTORE DE ATAQUE

3.1. ¿QUÉ ES HACKING ÉTICO?

El hacking ético es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de “pentester”. A la actividad que realizan se le conoce como “hacking ético” o “pruebas de penetración”.

Las pruebas de penetración surgieron como respuesta a la presencia y realización de los primeros ataques informáticos a las organizaciones, los cuales trajeron graves consecuencias, como pérdidas monetarias y de reputación. Es aquí donde interviene el trabajo de un “hacker ético”, ya que su labor es buscar vulnerabilidades en los sistemas de la organización para, posteriormente, poder mitigarlos y evitar fugas de información sensible.

El hacking ético, también es conocido como prueba de intrusión o pentest, se define esencialmente como el ``arte´´ de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.

3.2. TIPOS DE HACKER.

3.2.1. Black Hats.

Un black hat o hacker de sombrero negro es una persona que disfruta de penetrar en los sistemas de seguridad con la finalidad de realizar algún daño o crear software dañino (Malware).

3.2.2. White Hats.

Por el contrario de un black hat, los hackers de sombrero blanco son expertos en seguridad, quienes tienen una ética muy alta y utilizan sus conocimientos para evitar actividades ilícitas, analizan las vulnerabilidades de los sistemas y mejoran las seguridades de los mismos.

3.2.3. Gray Hats.

En contraste al Black y White Hat el hacker de sombrero gris, no se preocupa mucho por la ética, sino por realizar su trabajo, si necesita alguna información o herramienta y para ello requieren penetrar en un sistema de cómputo, lo hace, además disfruta poniendo a prueba su ingenio contra los sistemas de seguridad, sin malicia y difundiendo su conocimiento, lo que a la larga mejora la seguridad de los sistemas. Según su capacidad técnica se dividen en el hacker estándar y el "elite".

3.3. ETAPAS DE HACKING.

El hacking ético se realiza básicamente en 6 pasos cada uno de ellos detallado a continuación:

1. FootPrint o reconocimiento

Footprint es el acto de recopilación de información acerca de un sistema informático y de las empresas a las que pertenece. Este es el primer paso dado por los hackers para penetrar un sistema informático o una red.

Este paso es muy importante ya que se debe tener muy clara toda la información previa sobre el sistema al que se va a atacar.

2. Scanning y enumeración

El segundo paso del hacking ético y las pruebas de penetración implica dos términos que son la exploración o escaneo de puertos y la enumeración.

El escaneo de puertos es una técnica común usada por hacker para averiguar las puertas abiertas, se utiliza descubrir las vulnerabilidades en el listado de servicios de un puerto.

Por otra parte la enumeración es el primer ataque contra la red de destino, la enumeración es el proceso de reunir la información sobre un equipo de destino mediante la conexión de forma activa a la misma, se usa para identificar cuentas de usuario, cuenta del sistema y la cuenta de administrador.

3. Análisis de vulnerabilidades

El análisis de vulnerabilidades se subdivide en dos tipos interno y externo.

El interno se trata de pruebas de penetración desde la red interna que identifican los riesgos de las redes y sistemas internos, demostrando lo que podría hacer un usuario que ha ganado acceso a la red, simulando ser un usuario interno malintencionado. Este tipo de pruebas son muy interesantes pues estudios realizados sobre la seguridad de la información demuestran que alrededor del 80 al 90% de las violaciones de seguridad se originan desde usuarios internos;

Y el externo se trata de pruebas de penetración desde internet que identifican los riesgos de la red perimetral (es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.) y analizan si estos pueden ser utilizados para acceder a su red, violando sus medidas de seguridad, y en tal caso examinar si se produce el debido registro de lo que está sucediendo y si se accionan o no las alertas apropiadas, verificando la efectividad de los firewalls, de los sistemas de detección de intrusos (IDS), de los sistemas operativos y de los dispositivos de comunicaciones visibles desde Internet.

4. ***Obtención de acceso***

La obtención de acceso se refiere al ataque propiamente dicho, independientemente de la metodología utilizada en este punto se consiguió ya cumplir con un objetivo, la obtención de una o más contraseñas.

5. ***Escalamiento de privilegios.***

Este punto se lo conoce también como “Mantener el acceso”, la idea es blindar el sistema contra otros posibles hackers protegiendo las puertas traseras.

6. ***Borrado de huellas***

Luego de realizar una penetración a cualquier sistema, quedan rastros de los procesos que se realizaron, la idea del borrado de huellas es no ser descubierto para lo cual el hacker borra logs de acceso, logs de sistema, webshells, backdoors, etc. De esta manera se protege en caso de una investigación.

3.4. VECTORES DE ATAQUE ELASTIX.

3.4.1. ATAQUES EXTERNOS.

Los ataques externos se refieren a los que pueden realizarse desde internet es decir fuera de la red local, en el caso de las centrales Elastix estos ataques pueden realizarse a en sus 3 componentes: Linux, Asterisk y en sus aplicaciones WEB, así:

- Linux
    - Password cracking al servicio SSH
    - Revelación de la configuración vía SNMP
- Asterisk
    - Enumeración de entidades SIP
    - SIP Brute force attack a entidades SIP
    - Conexiones AMI

- Aplicaciones WEB
    - SQL inyección
    - Cross Site Scripting o XSS
    - Exploits

3.4.2. ATAQUES INTERNOS.

En el caso de los ataques internos, que son aquellos que pueden realizarse desde la red local, en el caso de Elastix tenemos dos posibilidades:

- Arp poisoning
- Captura de tráfico de voz

CAPÍTULO IV: DETERMINACION DE HARDWARE Y SOFTWARE NECESARIOS PARA REALIZAR UN PENTEST (E.H.)

4.1. TIPOS DE PLATAFORMA ELASTIX

4.1.1. Elastix appliances

Los Elastix appliances, son hardwares diseñados especialmente para garantizar el tráfico de llamadas requerido por el software Elastix, los cuales poseen características como:

- Diseño compacto: Son portátiles y de fácil mantenimiento, poseen accesibilidad a expansiones mediante puertos PCI o USB, son montables en racks.
- Bajo consumo de energía: Contribuyen en gran manera tanto con la disminución de costos de las empresas como con la conservación del medio ambiente.
- Capacidad de integración digital y analógica: Gracias a la accesibilidad a expansiones se puede integrar tarjetas digitales o analógicas (FXO/FXS, E1/T1), de acuerdo a los requerimientos.

Actualmente Elastix posee 4 tipos de appliances:

FIGURA 7: ELASTIX APPLIANCES (MINIUCS – ELX025)

FIGURA 8: ELASTIX APPLIANCES (NLX4000 – ELX5000)

En la siguiente tabla podemos observar las características que posee cada uno de estos appliances.

Descripción	miniUCS	ELX025	NLX4000	ELX5000
Puertos Analógicos	Hasta 8	Hasta 12	Hasta 48	Hasta 72
Puertos Digitales	Hasta 1 E1/T1/J1 ó 4 BRI	Hasta 1 E1/T1/J1	Hasta 4 E1/T1/J1	Hasta 8 E1/T1/J1
Slots de expansión PCI	1 PCIe	1 PCI	2 PCIe - easy swap	5: 1 PCI, 4 PCIe
Extensiones (SIP/IAX)	Hasta 50	Hasta 100	Hasta 300	Hasta 600
Llamadas concurrentes (max. Recomen.)	Hasta 32	Hasta 50	Hasta 120	Hasta 250

TABLA 1: COMPARACIÓN ELASTIX APPLIANCES

4.1.2. Elastix on Server/PC

El software de Elastix también nos proporciona la opción de ser instalado en equipos PC, Servidores, o usando opciones virtualizadas.
Para ello únicamente el hardware elegido debe cumplir con los requerimientos mínimos solicitados por el software que son:

- Disco Duro: 4GB
- Memoria RAM: 256MB

Es evidente que estos requisitos son fácilmente alcanzables, en cuyo caso los requisitos de hardware estarían dados más por el uso que se le dará al software instalado que los que éste necesita para funcionar.

Como ya hemos mencionado Elastix es un software OpenSource y se puede lo puede descargar directamente de su página oficial www.elastix.org, en la sección Descargas, en sus versiones de 32 y 64 Bits.
Para el desarrollo de éste proyecto de titulación se toma esta opción como la más viable, ya que puede y será instalado en una plataforma virtual.

4.2. SOFTWARE PARA HACKING ÉTICO

4.2.1. Kali Linux

Kali Linux es la nueva generación de la distribución Linux BackTrack para realizar Auditorías de Seguridad y Pruebas de Penetración, está basado en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.
Sus principales características son:

- Más de 300 herramientas de Pruebas de Penetración
- Es Libre y siempre lo será
- Árbol Git Open Source
- Cumple con FHS (Filesystem Hierarchy Standart)
- Amplio soporte para dispositivos inalámbricos
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro
- Paquetes y repositorios firmados con GPG
- Varios lenguajes

- Completamente personalizable
- Soporte ARMEL y ARMHF

Kali Linux posee algunas herramientas específicas que serán usadas en las pruebas de penetración entre ellas: nmap, rsmangler, hydra, svmap, svwar, svcrack.

NMAP

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Sus principales características son:

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking.

Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales.

Nmap permite hacer el inventario y el mantenimiento del inventario de computadores de una red. Se puede usar entonces para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte.

Nmap es a menudo confundido con herramientas para verificación de vulnerabilidades como Nessus. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

RSMANGLER

RSMangler es un script desarrollado en Ruby por la compañía de seguridad RandomStorm (los mismos creadores del DVWA – Damn Vulnerable Web App), que tomando como base una lista de palabras y realizando sobre cada una varias manipulaciones logra obtener un diccionario mucho más completo que el original, para utilizarlo en nuestras herramientas.

Supongamos que estamos realizando un pentest a una página web y queremos entrar a su servidor FTP por medio de fuerza bruta (usando los diccionarios que ya hemos publicado), después de mucho tiempo, nuestra herramienta termina de probar todas las combinaciones, pero no da con la clave, ¿qué hacemos?, sencillo usamos la herramienta RSMANGLER para generar nuestro propio diccionario.

Para tener una breve idea de qué tan grande puede ser un diccionario credo con RSMANGLER tomaremos como ejemplo generarlo a partir de 3 palabras, entonces el resultado será un diccionario con 4245 palabras, si lo hacemos con 5 palabras el diccionario tendrá 91975 palabras, de esta manera contamos con una herramienta poderosa para nuestros ataques por fuerza bruta.

HYDRA

Hydra es una herramienta que nos permite realizar ataques de fuerza bruta con diccionario, la cual nos posibilita el poder jugar con ella para intentar acceder a otros sistemas y automatizar intentos de login.

Ésta herramienta nos permite realizar intentos de login simultáneos y continuos, es parametrizable en cuanto al protocolo, número de intentos, intentos simultáneos y por su puesto el diccionario que queremos usar.

SVMAP

Svmap es un escáner de red para SIP. Similar a Nmap, su objetivo es buscar los dispositivos SIP de acuerdo a lo indicado en línea de comandos. Una vez svmap encuentra un dispositivo que soporte SIP, extraerá la información de la respuesta e identificará el tipo de dispositivo. Cualquiera que utilice esta herramienta típicamente va a terminar con una lista de direcciones IP de los dispositivos SIP y los nombres para esos dispositivos.

SVWAR

Svwar es una herramienta que nos permite obtener usuarios disponibles dentro de una PBX o servidor de VoIP.

El funcionamiento es bastante sencillo, svwar prueba con una serie de números por defecto, buscando en los siguientes rangos: 1000,2000... 9000, 1001, 2001..9001, 1111,2222... 9999, 11111,22222...99999, 100-999, 1234,2345 ..7890. Así es posible identificar extensiones en varias configuraciones del PBX. Adicionalmente svwar envía una respuesta ACK a las respuestas SIP con código 200 porque varios PBX continúan enviando paquetes hasta que reciben una confirmación.

SVCRACK

Ésta herramienta funciona de manera similar que Hydra, pero exclusivamente para contraseñas SIP, su objetivo es realizar un ataque de fuerza bruta para obtener la contraseña SIP de un determinado usuario usando un diccionario.

Es evidente que KALI Linux es el más indicada para el desarrollo del presente proyecto ya que cual se podrá trabajar de una forma más ágil y automatizada aprovechando cada una de sus herramientas.

4.3. SOFTWARE PARA VIRTUALIZACIÓN

4.3.1. Virtualbox

Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como sistemas invitados, dentro de otro sistema operativo anfitrión, cada uno con su propio ambiente virtual.

Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp, Microsoft Windows, y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros.

La aplicación fue inicialmente ofrecida bajo una licencia de software privativo, pero en enero de 2007, después de años de desarrollo, surgió VirtualBox OSE (Open Source Edition) bajo la licencia GPL 2. Actualmente existe la versión privativa Oracle VM VirtualBox, que es gratuita únicamente bajo uso personal o de evaluación, y está sujeta a la

licencia de "Uso Personal y de Evaluación VirtualBox" (VirtualBox Personal Use and Evaluation License o PUEL) y la versión Open Source, VirtualBox OSE, que es software libre, sujeta a la licencia GPL.

VirtualBox ofrece algunas funcionalidades interesantes, como la ejecución de máquinas virtuales de forma remota, por medio del Remote Desktop Protocol (RDP), soporte iSCSI, aunque estas opciones no están disponibles en la versión OSE.

En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas anfitriones como archivos individuales en un contenedor llamado Virtual Disk Image, incompatible con los demás softwares de virtualización.

Otra de las funciones que presenta es la de montar imágenes ISO como unidades virtuales ópticas de CD o DVD, o como un disquete.

Tiene un paquete de controladores que permiten aceleración en 3D, pantalla completa, hasta 4 placas PCI Ethernet (8 si se utiliza la línea de comandos para configurarlas), integración con teclado y ratón.

4.3.2. VMWare Workstation

VMware Workstation es un hipervisor que permite a los usuarios configurar una o más máquinas virtuales (VM) en una única máquina física, y los utilizan de forma simultánea junto con la máquina real. Cada máquina virtual puede ejecutar su propio sistema operativo, incluidas las versiones de Microsoft Windows, Linux, BSD, y MS-DOS. VMware Workstation es desarrollado y vendido por VMware, Inc., una división de EMC Corporation.

VMware Workstation es compatible con conexiones de red tipo bridge, nat, y host only; y posee la característica de compartir unidades de disco físico y dispositivos USB con una máquina virtual. Además, se puede simular las unidades de disco. Se puede montar un archivo de imagen ISO existente en una unidad de disco óptico virtual para que la máquina virtual lo vea como uno físico.

VMware Workstation puede guardar el estado de una máquina virtual (snapshot) en cualquier momento y se pueden usar después, teniendo la máquina virtual, el sistema operativo y todo software instalado en él de forma idéntica a cuando se realizó el snapshot.

Incluye la posibilidad de designar a múltiples máquinas virtuales opciones de encendido, apagado, suspendido o reanudado de forma automática, por lo que es especialmente útil para entornos de pruebas de cliente-servidor.

CAPÍTULO V: PRUEBAS DE PENETRACIÓN Y ANÁLISIS DE RESULTADOS

5.1. PRUEBAS DE PENETRACIÓN

5.1.1. Pentests

5.1.1.1. Footprint o reconocimiento

Para realizar el reconocimiento de la central se puede usar herramientas básicas como ping o whois, de esta manera identificaremos la dirección IP que corresponde al dominio que deseamos atacar

En este se realiza la prueba de ataque sobre la central IP con dominio odbk.com.ec, procederemos desde el terminal de kali linux realizando un ping al dominio indicado:

```
root@kali:~# ping odbk.com.ec
PING odbk.com.ec (192.168.1.50) 56(84) bytes of data.
64 bytes from odbk.com.ec (192.168.1.50): icmp_req=1 ttl=64 time=64.8 ms
64 bytes from odbk.com.ec (192.168.1.50): icmp_req=2 ttl=64 time=2.57 ms
64 bytes from odbk.com.ec (192.168.1.50): icmp_req=3 ttl=64 time=4.55 ms
64 bytes from odbk.com.ec (192.168.1.50): icmp_req=4 ttl=64 time=2.18 ms
64 bytes from odbk.com.ec (192.168.1.50): icmp_req=5 ttl=64 time=2.20 ms
```

FIGURA 9: DESCUBRIENDO DIRECCIÓN IP DE UN DOMINIO

Como se puede evidenciar hemos obtenido la dirección IP 192.168.1.50 correspondiente al dominio con la cual trabajaremos en adelante.

Después de obtener la dirección IP el siguiente paso es identificar a qué tipo de sistema operativo vamos a atacar y los puertos que están abiertos para poder realizar las pruebas de penetración. Este paso lo podemos realizar a través de la herramienta nmap ejecutándola de desde el terminal.

Seteamos el comando con las opción –A que habilita el análisis de sistema operativo y versión.

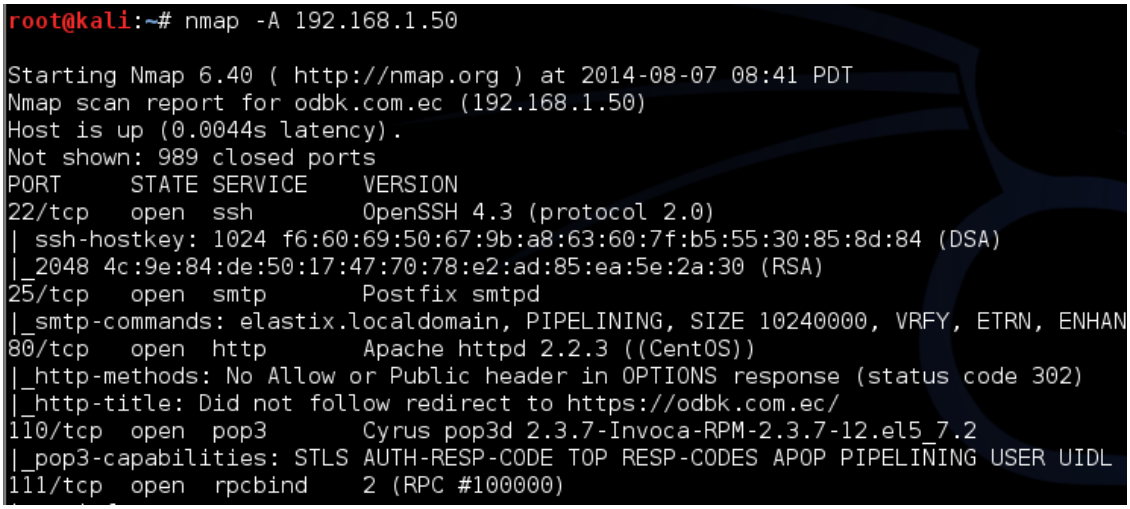


FIGURA 10: RESULTADOS OBTENIDOS USANDO NMAP (PARTE 1)

En esta primera parte de la captura se puede observar que el sistema operativo es Centos y los puertos 22, 25, 80 110 y 111 están abiertos.

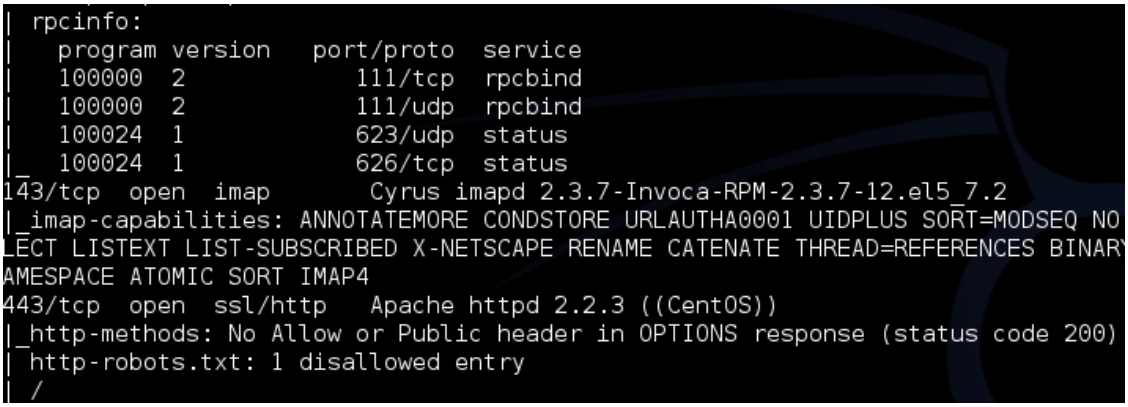


FIGURA 11: RESULTADOS OBTENIDOS USANDO NMAP (PARTE 2)

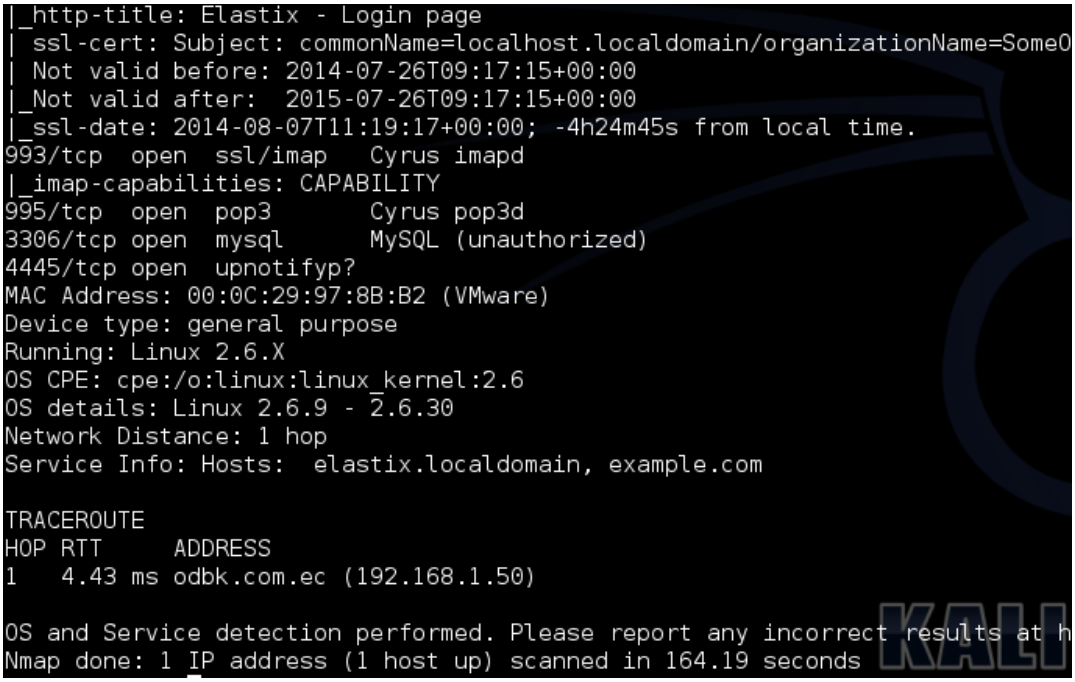


FIGURA 12: RESULTADOS OBTENIDOS USANDO NMAP (PARTE 3)

En las imágenes precedentes observamos el resto de puertos y servicios abiertos en esta central los cuales son: 143, 443, 993, 995, 3306, 445.

Los puertos y servicios encontrados serán listados en la tabla siguiente:

Puerto	Servicio	Versión	Estado
22	ssh	Open ssh 4.3	Abierto
25	smtp	Postfix smtpd	Abierto
80	http	Apache httpd 2.2.3	Abierto
110	pop3	Cyrus pop3d 2.3.7	Abierto
111	rcpbind	2	Abierto
143	imap	Cyrus imapd 2.3.7	Abierto
443	ssl/http	Apache httpd 2.2.3	Abierto
993	ssl/imap	Cyrus imapd	Abierto
995	ssl/pop3	Cyrus popd	Abierto
3306	MySQL	No reconocido	Abierto
445	No reconocido	No reconocido	Abierto

TABLA 2: LISTADO DE PUERTOS ENCONTRADOS CON NMAP

De esta manera podemos tomar una decisión para realizar las pruebas de penetración.

5.1.1.2. Identificación de dispositivos sip.

Para empezar la identificación de dispositivos usaremos la herramienta svmap, con la cual obtendremos información básica acerca de la central a la que estamos atacando.

```
root@kali:/tesis# svmap 192.168.1.50
| SIP Device          | User Agent             | Fingerprint |
-------------------------------------------------------------
| 192.168.1.50:5060 | FPBX-2.8.1(1.8.11.0) | disabled    |
```

FIGURA 13: IDENTIFICACIÓN DISPOSITIVOS SIP CON SVMAP

Como podemos observar el resultado del comando svmap nos indica que se está usando el puerto 5060 y la versión de PBX es FreePBX 2.8.1. Ésta información ya es una vulnerabilidad ya que se puede empezar una investigación especifica de las vulnerabilidades de la versión 2.8.1 de FreePBX.

5.1.1.3. Robo de contraseñas.

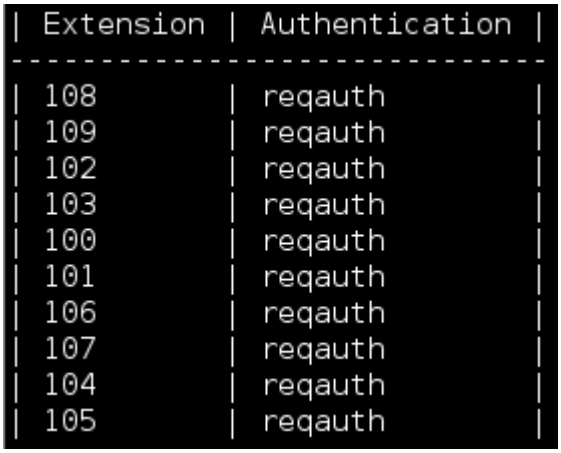
El primer paso será identificar los usuarios a los que podemos atacar dentro de la central IP, para ello usamos la herramienta svwar de la siguiente manera:

```
root@kali:/tesis# svwar -m INVITE --force 192.168.1.50
```

FIGURA 14: SINTAXIS HERRAMIENTA SVWAR

Aquí indicamos que realice una invitación de llamada a los usuarios de la central 192.168.1.50, es importante indicar que en este proceso es probable que las extensiones de los usuarios timbren cuando se acierta a una invitación.

De la ejecución de esta herramienta obtenemos el siguiente resultado:



Extension	Authentication
108	reqauth
109	reqauth
102	reqauth
103	reqauth
100	reqauth
101	reqauth
106	reqauth
107	reqauth
104	reqauth
105	reqauth

FIGURA 15: LISTADOS DE EXTENSIONES DISPONIBLES

De esta manera hemos listado las extensiones, por ende usuarios de los que podemos empezar a obtener las contraseñas.

Ahora para iniciar el robo de contraseñas necesitamos un diccionario de palabras para poder probar una a una, en este caso tenemos dos opciones podemos descargar un diccionario de internet, ya que existen millones de ellos, o también podemos generar nuestro propio diccionario utilizando la herramienta rsmangler de la siguiente manera:

Primero creamos un archivo con extensión “txt”:

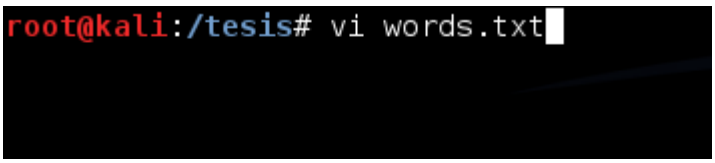


FIGURA 16: CREACIÓN ARCHIVO TXT PARA DICCIONARIO

Dentro de este archivo colocaremos las palabras con las que queremos que la herramienta rsmangler genere nuestro diccionario, el éxito de nuestro ataque depende mucho de las palabras que usemos.

FIGURA 17: CONTENIDO ARCHIVO TXT PARA DICCIONARIO

En este caso se colocan palabras comunes relacionadas con la central y el dominio que usan para su funcionamiento.

Ahora crearemos un segundo archivo y lo dejaremos en blanco, lo usaremos para guardar en el todas las palabras generadas por la herramienta rsmangler.

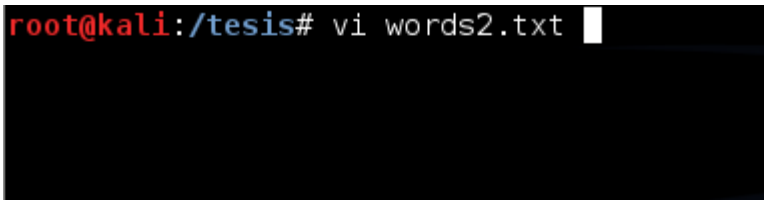


FIGURA 18: ARCHIVO TXT PARA PALABRAS GENERADAS

En este momento estamos listos para generar nuestro diccionario con la herramienta rsmangler y lo haremos de la siguiente manera:

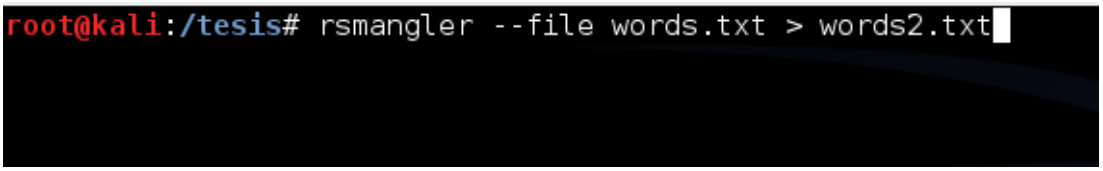


FIGURA 19: CREANDO DICCIONARIO CON RSMANGLER

Indicamos al comando que cree el diccionario con las palabras del archivo “word.txt” y lo almacene en el archivo “word2.txt”.

A partir de este momento usaremos el archivo “word2.txt” como nuestro diccionario para los ataques por fuerza bruta.

Veamos una parte del contenido de este archivo:

FIGURA 20: CONTENIDO ARCHIVO DE DICCIONARIO

Como se puede ver el archivo contiene una serie de combinaciones de las palabras que nosotros indicamos entre ellas y con opciones comunes usadas para contraseñas.

Ahora estamos listos para realizar un ataque por fuerza bruta y obtener la clave SIP de alguno de los usuarios identificados anteriormente.

Para esto usaremos la herramienta svcrack así:

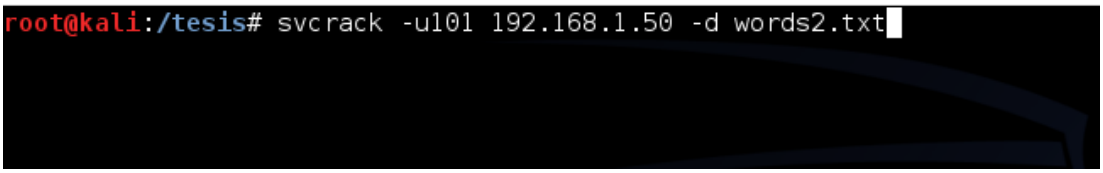


FIGURA 21: SÍNTAXIS COMANDO SVCRACK

Indicamos al comando svcrack que al usuario (extensión) 101 de la central 192.168.1.50 intente encontrar la contraseña basándose en el diccionario “word2.txt”

El resultado obtenido de este ataque es:

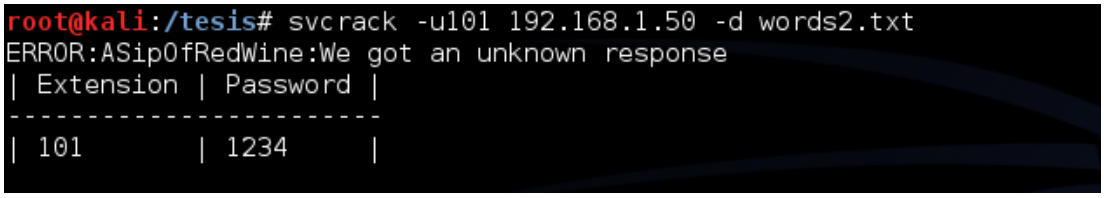


FIGURA 22: RESULTADOS HERRAMIENTA SVCRACK

Como vemos existe una coincidencia dentro de nuestro diccionario para esta extensión, con ello ya tenemos identificado el usuario y contraseña: “usuario: 101”, “contraseña:1234”, en este momento ya podemos usar esta extensión para realizar llamadas.

Con estos ataques hemos accedido con facilidad a la contraseña SIP de un usuario de la central. Sin embargo aún podemos realizar un ataque mucho más peligroso, en el listado de puertos identificado anteriormente visualizamos que el puerto 22 protocolo ssh se encuentra abierto, entonces podemos realizar un ataque para obtener acceso completo a la central IP y no únicamente a su PBX.

Para este ataque usaremos la herramienta Hydra, de la siguiente manera:

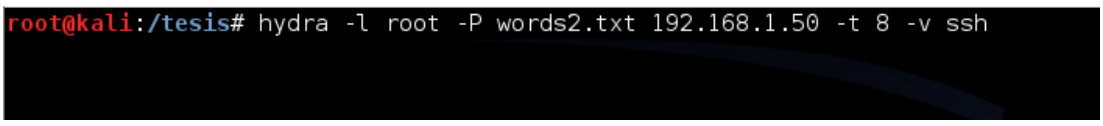


FIGURA 23: SINTAXIS COMANDO HYDRA

Aquí indicamos que inicie un ataque al usuario “root” de la central “192.168.1.50”, con las palabras del diccionario “word2.txt” realizando “8” intentos a la vez sobre el servicio “ssh”. El resultado de este ataque lo vemos en la siguiente figura:

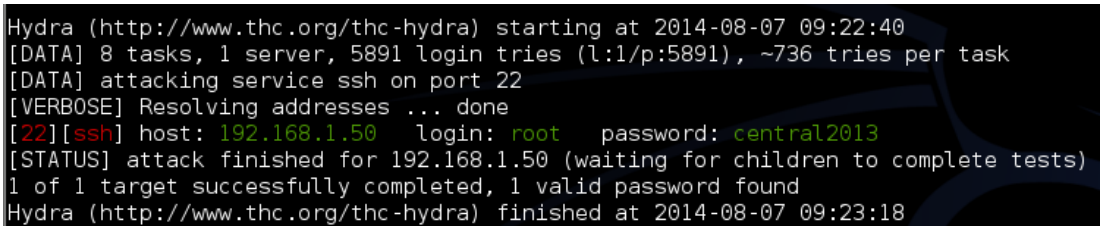


FIGURA 24: RESULTADOS HERRAMIENTA HYDRA

Como vemos en la figura se obtuvo la coincidencia entre usuario y contraseña con las palabras de nuestro diccionario. “usuario: root”, “contraseña: central2013”.

Con este ataque hemos conseguido acceso total a la central a través del servicio ssh en el puerto 22.

5.1.1.4. Denegación de servicios (DOS, DDOS)

En seguridad informática, un ataque de denegación de servicios, también llamado ataque DoS (de las siglas en inglés Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Para el caso de centrales IP esta denegación de servicios supone la falta de servicio a usuarios por demasiadas llamadas concurrentes.

Para ello utilizaremos el comando INVITEFLOOD.

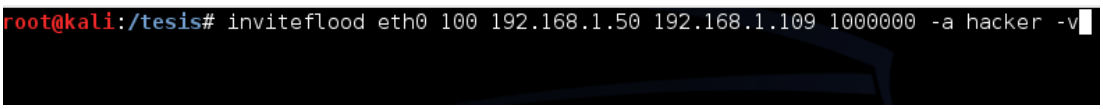


FIGURA 25: SÍNTAXIS COMANDO INVITEFLOOD

En este caso le indicamos al comando que procesa el ataque por la interfaz de red ETH0 a la extensión número 100 de la central con IP 192.168.1.50 desde la IP 192.168.1.109, realizara este flujo continuo

1000000 de veces y lo hará con el alias hacker, como resultado obtenemos:

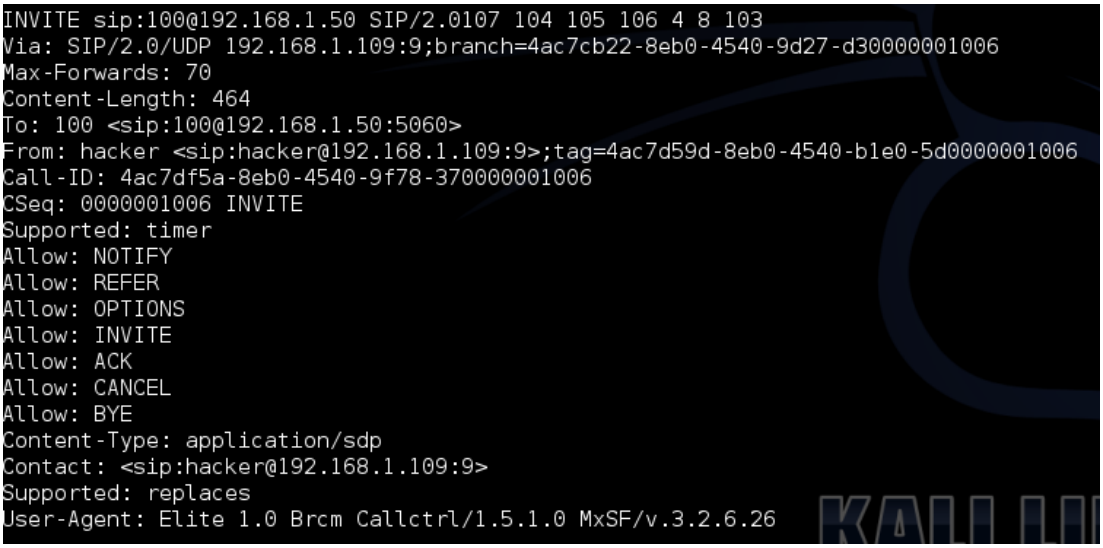


FIGURA 26: RESULTADO COMANDO INVITEFLOOD

Como resultado después del flujo concurrente de llamadas el usuario con extensión 100 ya no puede recibir ni realizar llamadas.

5.1.2. Resumen de vulnerabilidades.

La siguiente tabla resume las vulnerabilidades encontradas:

Número	Vulnerabilidad
1	Puertos innecesarios abiertos
2	Enumeración de dispositivos SIP habilitada.
3	Permisos de escaneo de usuarios habilitado
4	Robo de contraseñas de usuario por ataque de fuerza bruta permitido
5	Contraseñas usuarios débiles y muy intuitivas
6	Protocolo ssh sin protección
7	Contraseña de root débil.
8	Permiso de solicitudes concurrentes ilimitado
9	Firewall deshabilitado
10	Servicios no utilizados, habilitados

TABLA 3: RESUMEN DE VULNERABILIDADES

5.1.3. Análisis de Vulnerabilidades.

1. ***Puertos innecesarios abiertos:***

Este tipo de vulnerabilidad es muy común cuando se realiza una instalación desatendida o por defecto, la mayoría de usuarios desconoce los problemas que se pueden generar al dejar estos puertos abiertos. Para un hacker un puerto abierto es semejante a una puerta de casa abierta para un ladrón.

Los puertos abiertos permiten el inicio de los ataques, quizá no todos los puertos sean vulnerables pero implican un riesgo ya que con el análisis apropiado incluso un puerto de correo pude convertirse en una vulnerabilidad para una central IP.

La solución más apropiada en este caso es cerrar los puertos innecesarios, podemos realizarlos a través de la configuración manual de iptables o con la herramienta firewall de Elastix.

2. ***Enumeración de dispositivos SIP habilitados.***

Los problemas que ocasiona son evidentes, si una persona puede listar los dispositivos SIP que funcionan en una central es muy sencillo realizar una investigación a fondo de todas las vulnerabilidades que la versión de dispositivo tiene. Generalmente podemos encontrar estas vulnerabilidades en foros pertenecientes al mismo fabricante, la gente normalmente reporta este tipo de errores para que en una próxima versión el fabricante la corrija, sin embargo la buena intención de estas personas es una herramienta poderosa para los hackers.

Además de ellos conocer la versión exacta nos da la posibilidad de recrear un escenario similar al que queremos atacar y encontrara vulnerabilidades para luego aplicarlas en la víctima real.

Para solucionarlo podemos implementar reglas de acceso en el Firewall que viene preinstalado en el sistema operativo pero no está configurado.

3. ***Permisos de escaneo de usuarios habilitado.***

   Ésta vulnerabilidad ocurre debido a una configuración por defecto que trae la central Elastix, su solución es muy sencilla sin embargo el desconocimiento del mismo provoca que los usuarios puedan ser listados, lo que conlleva a que el atacante pueda escoger específicamente un usuario para un ataque más personalizado, sin lugar a dudas es una grave falla en la seguridad de nuestra central ya que un ataque der este tipo no solo pone en riesgo a nuestra plataforma sino también al usuario o usuarios que son atacados.

   Como mencione anteriormente la solución a esta vulnerabilidad es muy sencilla, basta con cambiar un parámetro dentro del archivo de configuración “sip.conf”

4. ***Robo de contraseñas de usuario por ataque de fuerza bruta permitido.***

   Ésta vulnerabilidad va de la mano con la anterior, de igual manera se produce por la configuración por defecto de la central Elastix, es lógico darse cuenta que si este tipo de ataque es permitido un hacker podría tomarse el tiempo necesario y obtener las contraseñas de los usuarios, en el momento en que un hacker obtiene una contraseña está completamente habilitado para realizar llamadas gratuitas a través de la extensión del usuario atacado.

   La corrección de ésta va ligada a la anterior, al cambiar el parámetro en el archivo sip.conf se soluciona también.

5. ***Contraseñas usuarios débiles y muy intuitivas***

   El tema de contraseñas inseguras está relacionado directamente con una falta de cultura en seguridad informática, en los

principios de la computación las contraseñas más comunes eran DIOS, AMOR, SEXO, nombres de los usuarios y secuencias sencillas de números, con el paso del tiempo se fue haciendo muy necesario colocar claves más robustas. Sin embargo al configurar claves de centrales IP es muy común encontrarse con contraseñas como “1234 , 9876, asdf” y es por ello que al generar un diccionario de ataque las contraseñas son fácilmente encontradas.

Este error de seguridad recae directamente sobre la persona encargada de crear las extensiones y contraseñas, muchas veces colocan claves sencillas para facilidad de los usuarios, pero ya podemos ver que no es lo correcto si deseamos un estándar de seguridad alto en nuestra central IP.

La solución se da implementando contraseñas más robustas y no intuitivas mientras menos relación tengan con el usuario es mejor.

6. Protocolo ssh sin protección

El protocolo SSH sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, en cuanto a seguridad trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

Es decir a pesar de tratarse de un protocolo más seguro que TELNET sigue siendo vulnerable a menos que sepamos protegerlo. En el caso específico del ataque que realizamos el problema se da porque nos permite ejecutar un ataque con varios usuarios concurrentes probando una y otra clave hasta dar con la correcta.

Para protegernos de mejor manera se debe evitar un número de usuarios concurrentes ilimitado y para eso también nos ayuda la herramienta FAIL2BAN.

7. Contraseña de root débil

Como ya mencionamos anteriormente el problema de contraseñas débiles se da por la falta de conocimiento en seguridad informática, sin embargo es mucho más grave encontrarnos con una contraseña de usuario root débil, debido que al acceder con este usuario el hacker tiene un control total sobre nuestra central.

En el caso específico que hemos analizado encontramos una contraseña fácil de recordar, relacionada con la plataforma utilizada y posiblemente el año en que fue implementada.

La solución sin lugar a dudas colocar contraseñas mucho más robustas y con un mayor criterio.

8. Permiso de solicitudes concurrentes ilimitado

Ésta vulnerabilidad se genera por un simple desconocimiento, es difícil imaginarse que alguien puede atacar a un usuario evitando que pueda utilizar su extensión telefónica. Pero hay que resaltar que un hacker con ganas o motivos para hacer daño puede valerse de cualquier cosa para atacar a sus víctimas.

Si ponemos un ejemplo podría tratarse de un gerente que esta fuera del país y utiliza su extensión SIP en su celular, si el hacker logra denegar los servicios podría generar un gran problema, estaría dejando al gerente de una empresa incomunicado por un periodo de tiempo desconocido.

9. Firewall deshabilitado

Un error muy común en el uso de centrales IP es no explotar todas las herramientas que posee, se cumple con claridad el principio

de “Pareto”, el cual da una relación de 80 – 20, en nuestro caso lo interpretaríamos como que el 20% de las herramientas que posee la central es usado por el 80% de usuarios y así mismo el 80% de herramientas es usado por apenas un 20% de usuarios.

Si la centra nos brinda un módulo de seguridad que incluye un Firewall es evidente y lógico que deberíamos usarlo para protegernos de una infinidad de ataques.

10. Servicios no utilizados, habilitados

Seguimos cometiendo el mismo error, por realizar instalaciones desentendidas o dejar todo por defecto, muchos servicios que no utilizamos los dejamos habilitados, lo que desencadena en vulnerabilidades para nosotros.

Un hacker puede ejecutar scripts específicos para cada uno de estos servicios y encontrar fallas en la seguridad, terminando nuevamente en un problema para nosotros.

La solución es muy clara, deshabilitar los servicios que no usamos, o aprovechar su uso pero protegiéndolos.

CAPÍTULO VI: IMPLEMENTACIÓN DE SOLUCIONES Y ANÁLISIS DE RESULTADOS

6.1. PLANTEAMIENTO DE SOLUCIONES A LAS VULNERABILIDADES ENCONTRADAS.

En el capítulo anterior fuimos determinando durante el análisis cuales serían las soluciones más apropiadas, en la siguiente tabla resumimos las mismas:

Número	Vulnerabilidad	Solución
1	Puertos innecesarios abiertos	Cerrar puertos innecesarios
2	Enumeración de dispositivos SIP habilitada.	Configurar reglas de acceso en Firewall
3	Permisos de escaneo de usuarios habilitado	Corregir valor por defecto en archivo sip.conf
4	Robo de contraseñas de usuario por ataque de fuerza bruta permitido	Corregir valor por defecto en archivo sip.conf
5	Contraseñas usuarios débiles y muy intuitivas	Implementar contraseñas más robustas.
6	Protocolo ssh sin protección	Configurar herramienta FAIL2BAN
7	Contraseña de root débil.	Implementar contraseñas más robustas
8	Permiso de solicitudes concurrentes ilimitado	Configurar herramienta FAIL2BAN
9	Firewall deshabilitado	Habilitar firewall propio de Elastix
10	Servicios no utilizados, habilitados	Deshabilitar servicios no usados.

TABLA 4: RESUMEN SOLUCIONES A IMPLEMENTAR

6.2. IMPLEMENTACIÓN SOLUCIONES.

Algunas de las soluciones propuestas están relacionadas unas con otras, así que procederemos en el siguiente orden:

1. Implementar contraseñas más robustas
2. Configurar herramienta FAIL2BAN
3. Habilitar firewall de Elastix

4. Cerrar puertos no usados y servicios de aplicaciones no utilizadas
5. Corregir archivo de configuración sip.conf

El orden lo elegimos de esta manera para demostrar que con una contraseña más robusta el proceso de hacking se vería mucho más demorado.

1. Implementar contraseñas más robustas

Empecemos, lo primero que haremos es cambiar la contraseña del súper usuario root, haciendo uso del comando passwd:

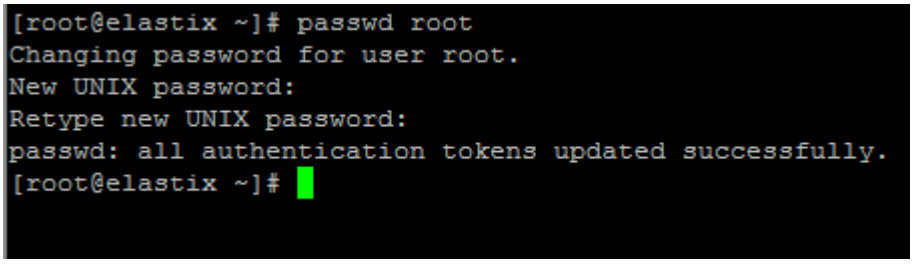


FIGURA 27: CAMBIO DE CONTRASEÑA ROOT

Ahora cambiaremos la clave de los usuarios o extensiones, esto lo podemos hacer en el modo gráfico de la central:

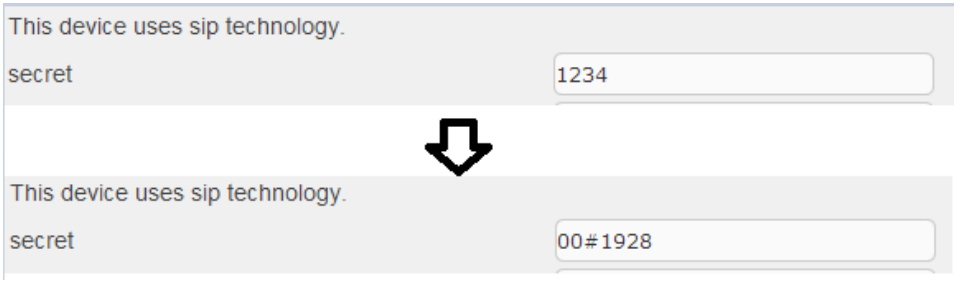


FIGURA 28: CAMBIO CONTRASEÑA USUARIOS

Una vez realizado este proceso realizaremos nuevamente ambas pruebas de penetración sin implementar ninguna de las otras soluciones. Los resultados se pueden ver en la siguiente sub capítulo.

2. Configurar herramienta FAIL2BAN

Para configurar esta herramienta seguiremos el tutorial del Anexo 1.

Es necesario verificar si la herramienta está instalada, para ello ejecutamos:

```
[root@elastix ~]# service fail2ban status
Fail2ban is stopped
[root@elastix ~]#
```

FIGURA 29: REVISAR ESTADO DE HERRAMIENTA FAIL2BAN

Si la respuesta al comando es la que vemos en la figura, la herramienta está instalada pero no se está ejecutando posiblemente porque no está configurada, si la respuesta obtenida es similar a "service fail2ban unrecognized" es necesario instalarla para lo cual usaremos la instrucción "yum install failt2ban".

Al finalizar el tutorial indicado podemos verificar nuevamente y obtendremos:

```
[root@elastix ~]# service fail2ban status
Fail2ban (pid 4968) is running...
```

FIGURA 30: HERRAMIENTA FAIL2BAN EN FUNCIONAMIENTO

3. Habilitar Firewall de Elastix

Para habilitar el firewall podemos ingresar al modo gráfico en la sección seguridad:

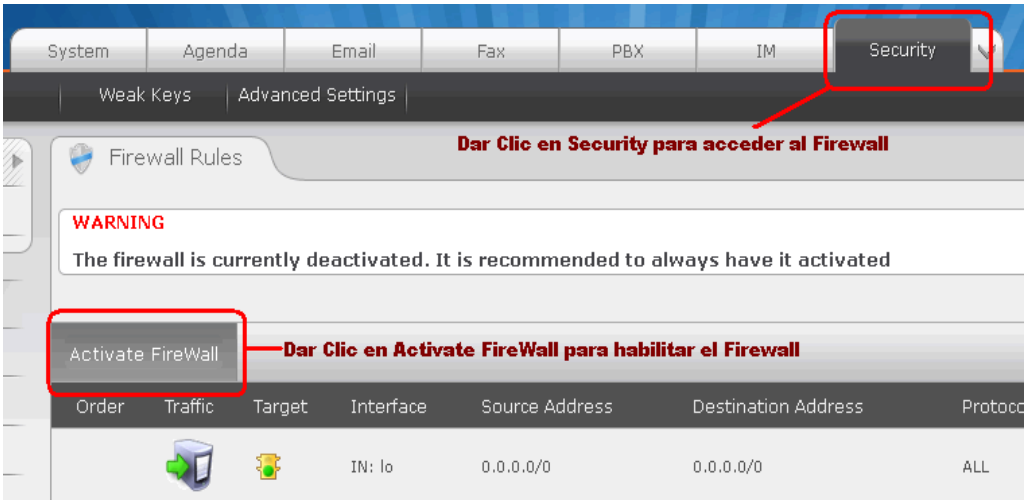


FIGURA 31: HABILITAR FIREWALL DE ELASTIX

Después de habilitarlo podemos ver un mensaje que nos indica que está activado y en la parte inferior las reglas creadas, las cuales modificaremos según nuestra conveniencia.

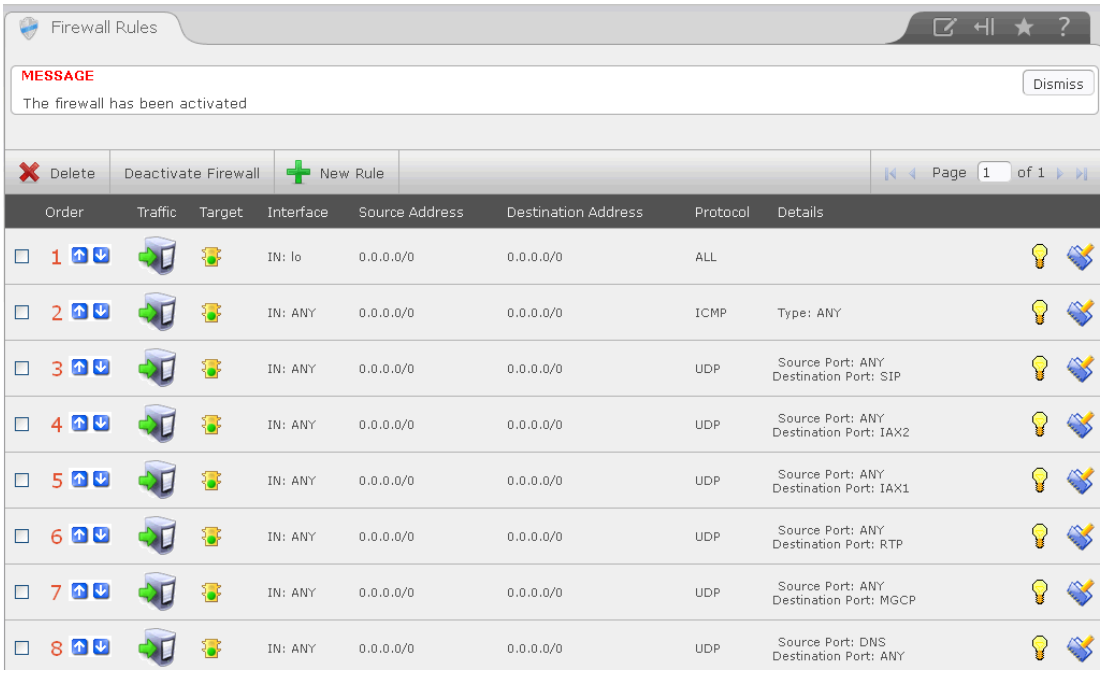


FIGURA 32: FIREWALL ACTIVADO, REGLAS DE ACCESO

4. *Cerrar puertos no usados y servicios de aplicaciones no usadas*

Este proceso lo podemos realizar desde el modo gráfico desactivando todos los puertos innecesarios. Dejaremos activos solo los necesarios que constan en la siguiente tabla:

Puerto	Protocolo	Descripción
22	TCP	Acceso remoto SSH
443	TCP	Acceso modo gráfico HTTPS
10000-20000	UDP	Comunicación SIP/RTP
5060	TCP/UDP	Comunicación SIP
4569	UDP	Comunicación IAX2

TABLA 5: PUERTOS NECESARIOS

5. Corregir archivo de configuración sip.conf

Finalmente vamos a cambiar el parámetro “alwaysauthreject” dentro del archivo sip.conf localizado en la ruta /etc/asterisk/sip.conf, así:

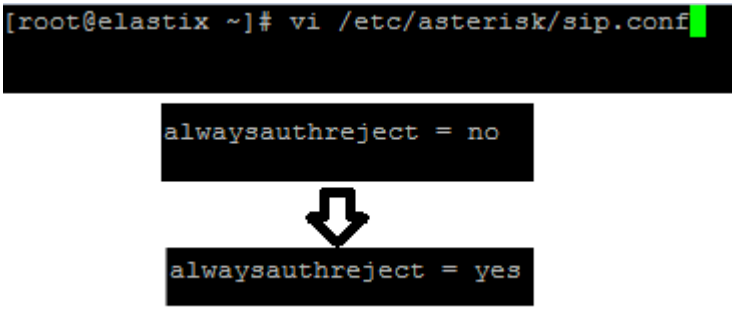


FIGURA 33: CAMBIO ARCHIVO SIP.CONF

De esta manera hemos implementado las soluciones correspondientes veamos que sucede a continuación con las pruebas de penetración.

6.3. PRUEBAS DE PENETRACIÓN.

Como indicamos anteriormente probaremos primero únicamente con el cambio de contraseñas:

Primero con la herramienta SVCRACK para descubrir las claves de los usuarios:

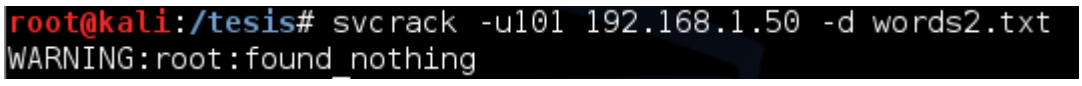


FIGURA 34: SVCRACK DESPUÉS DE CAMBIAR CONTRASEÑÁS

Ahora haremos lo mismo con la herramienta hydra para la clave del usuario root:

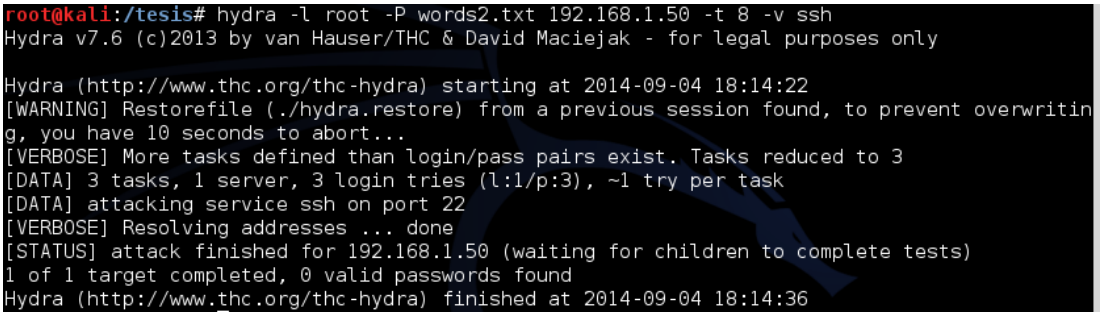


FIGURA 35: HYDRA DESPUES DE CAMBIAR CONTRASEÑA

En ambos casos vemos que el resultado es negativo para la coincidencia de contraseñas.

Ahora continuemos con el resto de ataques para determinar el resultado de las soluciones implementadas.

Veamos a continuación un nuevo escaneo con la herramienta NMAP:

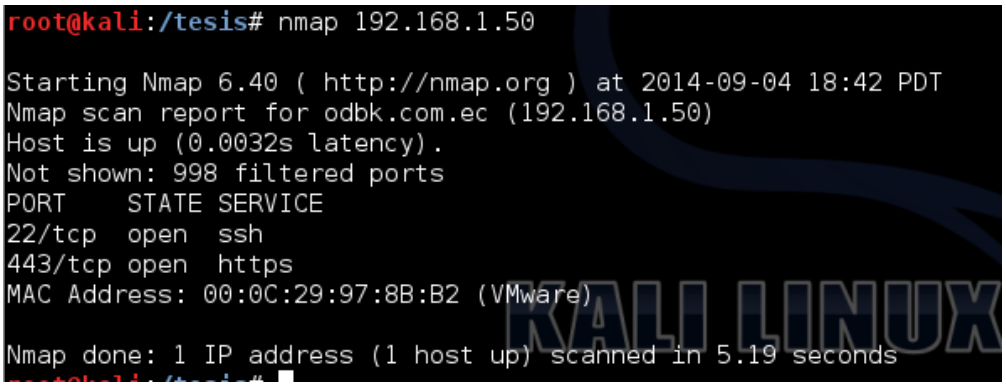


FIGURA 36: NMAP DESPUÉS DE CERRAR PUERTOS NO USADOS

Ahora la herramienta SVMAP para enumerar los dispositivos SIP y sus características:

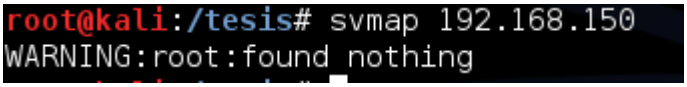


FIGURA 37: SVMAP DESPUÉS DE IMPLEMENTAR FIREWALL

Continuemos con la herramienta SVWAR para identificar las extensiones de usuarios:

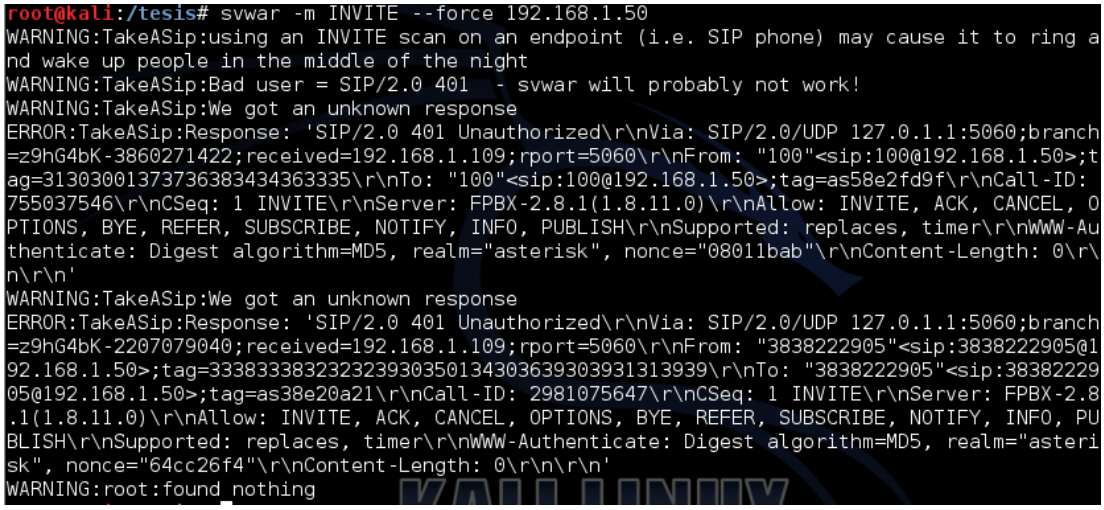


FIGURA 38: SVWAR DESPUÉS DE CORREGIR ARCHIVO SIP.CONF

Observemos lo que sucede al ejecutar la herramienta HYDRA con FAIL2BAN configurado:

FIGURA 39: HYDRA LUEGO DE IMPLEMENTAR FAIL2BAN

Como observamos en todas las imágenes hemos obtenido resultados positivos para corregir las vulnerabilidades encontradas.

6.4. ANÁLISIS DE RESULTADOS.

Para realizar el análisis luego de la implementación de las soluciones, haremos una comparación antes y después de las mismas por cada herramienta de Kali Linux usada, así:

Herramienta	Solución	Antes	Después
NMAP	Cerrar puertos y servicios no usados	Descubrió muchos puertos y servicios innecesarios habilitados	Detecto los puertos necesarios habilitados
SVMAP	Aplicar reglas de acceso en el Firewall	Determino la versión de dispositivo SIP usada	No encontró nada.
SVWAR	Corregir archivo sip.conf	Listo todas las extensiones de usuarios existentes	No listo nada
SVCRACK	Cambio contraseña	Detecto la clave correspondiente a la extensión 101	No pudo determinar contraseñas válidas
HYDRA	Cambio de contraseña	Detecto la clave del usuario root	No encontró coincidencias en contraseñas
HYDRA	Configuración FAIL2BAN	Pudo hacer pruebas con varias claves para el usuario root	El intento de encontrar la clave por fuerza bruta fue bloqueado

TABLA 6: RESULTADOS SOLUCIONES IMPLEMENTADAS

De esta manera vemos que los resultados han sido sumamente exitosos para la protección de nuestra central IP Elastix.

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

- El hacking ético aparece como una parte de una solución potencial para la mejorar la seguridad de los sistemas informáticos. El hacking ético trata de arreglar un sistema atacándolo en muchos casos con éxito.

  Un agujero de seguridad en informática no es sólo un problema referente a dañar hardware o software, también implica el riesgo de un daño a usuarios. Una planificación regular de auditorías más un sistema de detección de intrusos, más un buen sistema de prácticas administrativas, y herramientas de software de seguridad para los equipos son partes esenciales de la seguridad de una organización.

- Los beneficios de entrenar hackers éticos lejos de los riesgos asociados, tiene una finalidad muy precisa: contrarrestar el daño que puede causar un hacker malicioso en una organización de tal manera que las vulnerabilidades sean mitigadas antes de que sean explotadas. Pero es necesario un entrenamiento apropiado para formar un hacker “ÉTICO” como su palabra lo dice es un más complicado que solo formarlo en la parte teórico-práctica, sino también en la parte ética.

- Las fases seguidas por un hacker son muy ordenadas, y cada una de ellas requiere de una planificación correcta para evitar ser detectado, un hacker malicioso tiene por objetivo realizar su ataque y luego borrar toda huella que lo pueda comprometer, para ello se necesita mucha precisión y cuidado en el proceso.

- Gracias a las herramientas que nos provee Kali Linux se pudo determinar varias vulnerabilidades de las centrales Elastix, pero

cabe recalcar que la mayoría de ellas se producen por una falta de interés o conocimiento de las personas que implementa la central, puesto que son vulnerabilidades por realizar instalaciones desatendidas con valores por defecto.

- Las soluciones implementadas tuvieron un gran éxito logrando asegurar las vulnerabilidades encontradas, sin embargo es importante pensar que estas no son las únicas soluciones posibles, así como tampoco son todas las vulnerabilidades existentes.

- La mayoría de usuarios cometen el error de no utilizar adecuadamente las herramientas de seguridad que provee la propia plataforma, en muchos de los casos esas herramientas podrían evitar la vulnerabilidad de la central.

- Uno de los errores más evidentes es la falta de conciencia al momento de poner las contraseñas, generalmente los usuarios buscan claves fáciles de recordar o que están íntimamente relacionadas con cosas personales o con el sistema que están usando.

7.2. RECOMENDACIONES

- Al realizar una instalación de cualquier software o sistema operativo, es importante leer bien las opciones que estamos configurando por defecto, muchos de estas vienen por defecto para facilidad del usuario, pero eso no implica que se tome en cuenta la seguridad. Si tenemos la oportunidad y el conocimiento es mejor realizar una instalación lo menos desatendida posible

configurando desde el principio todos los parámetros de seguridad que fueren necesarios.

- Uno de los puntos más importantes resaltados a lo largo de este proyecto de tesis fue la falta de criterio para las contraseñas, es recomendable que dentro de una empresa se manejen políticas de seguridad en contraseñas, de esta manera todos los usuarios están al tanto de cómo crear una contraseñas robusta, e incluso este tema de seguridad debería ser parte de las capacitaciones que reciben los empleados nuevos.

- Elastix es una plataforma muy robusta y bastante segura si sabe implementar de la manera correcta, es importante leer los tutoriales y papers que se encuentran el su página oficial, muchos de ellos son enfocados específicamente a temas de seguridad, de esta forma evitaríamos contratiempos y explotaríamos de mejor manera las herramientas propias de la plataforma.

- Las herramientas de seguridad y vulnerabilidades cambian a diario. Cada día nuevas proezas son publicadas, además nuevas herramientas y scripts son implementadas o actualizadas. Debido a esto es importante mantenerse siempre actualizado para lo cual se puede acceder a una suscripción a sitios que brinden información relacionada con seguridad, lectura de revistas y papers. De esta manera podemos prevenir posibles ataques implementando nuevas herramientas de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

MATHEW, Thomas, Ethical Hacking and Countermeasures [EC-Council Exam 312-50] —Student Courseware, OSB Publisher © 2004.

WHITAKER, Andrew, NEWMAN Daniel. Penetration Testing and Network Defense, Cisco Press, USA, Noviembre 2005

www.telefoniavozip.com/voip/que-es-la-telefonia-ip.htm

www.pacifico.csic.es/uym3/soporte/help/termbody.html

es.wikibooks.org/wiki/Comunicaciones_Unificadas_Con_Elastix/Introducci%C3%B3n_a_la_VOZIP

elastixtech.com/puertos-tcp-udp-utilizados-en-elastix/

www.voipelia.com/freepbx-interfaz-usuario-asterisk/

es.wikipedia.org/wiki/Openfire

es.wikipedia.org/wiki/Servidor_HTTP_Apache

es.wikipedia.org/wiki/Vtiger_CRM

www.infoworld.com/d/virtualization/review-vmware-workstation-9-vs-virtualbox-42-203277

elastixtech.com/seguridad-básica-en-elastix/

liberatech.mx/2013/04/configurar-fail2ban-en-elastix-2-4-paso-a-paso/