Análisis de vulnerabilidades de seguridad en centrales VoIP Elastix a través de hacking ético

Julio Sotomayor, Ing. Carlos Romero, Ing. Fabián Saenz

Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejercito

Quito, Ecuador

jcsp_16@hotmail.com

Resumen: El presente artículo describe el análisis de vulnerabilidades de seguridad en centrales de VoIP Elastix usando como herramienta el hacking ético. En el análisis fue considerado el proceso que seguiría un hacker para obtener acceso a centrales Elastix, con la finalidad de buscar métodos que ayuden a prevenir este tipo de intrusiones. Al final de este proceso se determinaron las vulnerabilidades más peligrosas y sus respectivas soluciones.

I. INTRODUCCIÓN

El crecimiento de los avances tecnológicos nos ha permitido romper innumerables barreras en todo ámbito, principalmente a nivel de comunicaciones, la aparición de voz sobre IP determina un punto crucial en calidad y en costos bajos.

Sin embargo, con su uso, también se crea una brecha en la seguridad que este tipo de tecnología puede brindar a los usuarios. Si se analiza la necesidad de un usuario es fácil determinar que no usarían un medio de comunicación con el cual la confidencialidad de sus llamadas se ve en riesgo.

Entonces es lógico el énfasis en buscar los métodos que permitan preservar y asegurar la confidencialidad mediante altos estándares de seguridad. Para ello es necesario poner a prueba las plataformas que brindan este servicio para verificar si realmente pueden cumplir con nuestras expectativas, en este artículo nos centraremos específicamente en las centrales Elastix, que han tenido un crecimiento acelerado durante los últimos años y haremos uso del hacking ético para ponerla a prueba.

II. ANÁLISIS DE LA ESTRUCUTRA DE 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.

Sus principales protocolos de trabajo son: SIP, RTP, IAX, MGCP, SCCP y sus puerto comunes de trabajo son: 5060, 4569, y generalmente del 10000 al 20000.

A continuación observemos como ser realiza la comunicación en una llamada SIP y los puertos que utiliza.

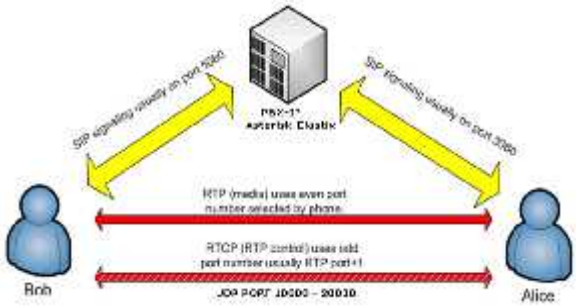

FIGURA 1: PUERTOS TCP/UDP UTILIZADOS POR SIP EN ELASTIX

Generalmente encontramos dos topologías de red principales para su uso la primera es una red estándar con una LAN y una WAN:

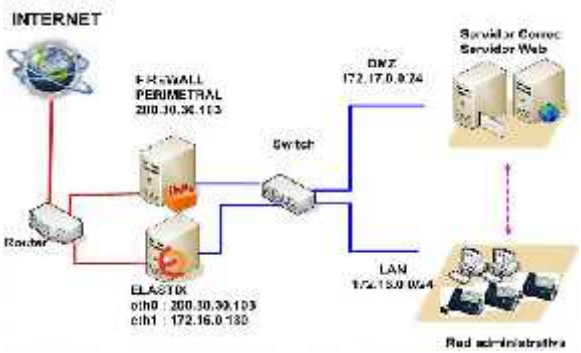

FIGURA 2: ELASTIX CON IP PÚBLICA + ESTÁTICA

Y la segunda con una plataforma virtual alojada en la nube a la cual los usuarios se conectan a través de internet:

FIGURA 3: ELASTIX EN LA NUBE

En ambos casos la central posee una dirección IP pública, la cual la convierte en un blanco para atacar.

III. 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 proceso que un hacker sigue se resume en 6 pasos que son:

- Footprint o reconocimiento: consiste en recopilar información sobre el sistema o plataforma a la que se va a atacar.
- Scanning y enumeración: en este paso el hacker determina que puertos pueden ser atacados y enumera los usuarios de los que se puede obtener información como claves de acceso.
- Análisis de vulnerabilidades: consiste en determinar las fallas de seguridad tanto internas (LAN) como externas (WAN) que posee la plataforma.
- Obtención de acceso: este punto es el ataque propiamente dicho, si este punto se consigue quiere decir que se obtuvo al menos una clave de acceso.

- Escalamiento de privilegios: se refiere a mantener el acceso que se ha conseguido, para que no pueda ser sacado del sistema, generalmente la idea es escalar al privilegio de administrador del sistema.
- Borrado de huellas: para un hacker el anonimato es primordial este paso consiste en borrar cualquier tipo de prueba que lo incrimine como por ejemplo los logs de acceso.

Entonces en nuestro caso para atacar una central Elastix existen dos opciones:

- Realizar un ataque externo, es decir desde fuera de la red local donde se encuentra en funcionamiento la central Elastix, lo cual es factible ya que no se necesita mayor información para iniciar este ataque.
- La segunda es un ataque interno, es decir dentro de su red local, a través de captura de tráfico con snifers y métodos similares, es factible solo si se tiene acceso a la red local.

IV. SOFTWARE NECESARIO

FIGURA 4: KALI LINUX

Para realizar un proceso de hacking existen muchas herramientas que se pueden obtener en internet, para nuestro caso la herramienta más completa es Kali Linux, el cual 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.

Dentro de él las herramientas que más nos interesan son las relacionadas con descubrimiento de red, ataques por fuerza bruta y ataques a dispositivos SIP.

Entre ellas las que más usaremos:

- NMAP: descubrir puertos y aplicaciones.
- RSMANGLER: generación de diccionarios para ataques por fuerza bruta.
- HYDRA: Ataques por fuerza bruta con uso de diccionarios.
- SVMAP: escaneo de dispositivos SIP.
- SVWAR: escaneo de usuarios y extensiones de centrales IP.
- SVCRACK: ataques por fuerza bruta a usuarios de la central.

V. PENTESTS (PRUEBAS DE PENETRACIÓN)

Para empezar con las pruebas de penetración es necesario seguir el proceso de hacking, empezando por el reconocimiento, para lo cual usamos el comando NMAP, su sintaxis es la siguiente:

nmap –(opción) (ip o dominio)

por ejemplo

nmap –A 192.168.1.50

La opción “-A” hace referencia a la palabra ALL en inglés, es decir nos entregará toda la información que pueda encontrar de la dirección que hemos solicitado.

En nuestro caso luego de ejecutar este comando se obtuvo la siguiente información relevante:

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

FIGURA 5: RESULTADOS COMANDO NMAP

Con esta información podemos determinar principalmente que el puerto 22 del protocolo ssh está abierto, y por las características de los servicios encontrados se trata de una central IP.

Entonces podemos proceder con el comando SVMAP para mapear dispositivos SIP, la sintaxis para el comando es:

svmap (ip o dominio)

por ejemplo

svmap 192.168.1.50

Es decir le pedimos que escanee esta dirección IP en busca de dispositivos SIP

Para lo cual nosotros obtuvimos:

192.168.1.50:5060 FPBX-2.8.1(1.8.11)

Es decir existe una central versión FPBX 2.8.1 funcionando en el puerto 5060, aquí ya encontramos una de las primeras vulnerabilidades, ya que con la versión de la central se puede realizar un estudio intensivo de formas para atacarla.

Continuando con las pruebas podemos utilizar ahora el comando SVWAR, para determinar si la central permite listar las extensiones telefónicas configuradas, su sintaxis es la siguiente:

svwar – (opción) - -(tipo de ataque) (ip o dominio)

por ejemplo

svwar –m INVITE - -force 192.168.1.50

Con ésta sintaxis le indicamos que realice una invitación de llamada por fuerza bruta a las extensiones que encuentre en la central con IP 192.168.1.50, el resultado obtenido fue:

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

FIGURA 6: RESULTADOS SVWAR

Entonces al momento ya conocemos las extensiones que están en funcionamiento en esta central.

El siguiente paso sería realizar ataques de fuerza bruta para descubrir las contraseñas de dichas extensiones, pero antes necesitamos un diccionario de palabras que utilizaremos para este ataque.

Los diccionarios de palabras son archivos de texto que contienen miles de palabras con las que la herramienta seleccionada

realizara los ataques, estos pueden ser descargados de internet, o generados con el comando RSMANGLER, su sintaxis es la siguiente:

rsmangler - -file (archivo1.txt) > (archivo2.txt)

por ejemplo

rsmangler - -file word.txt > word2.txt

El primer archivo word.txt debe contener las palabras clave con que queremos generar nuestro diccionario por ejemplo: “central, elastix, admin”, entonces el comando ejecuta la acción de realizar combinaciones con estas palabras y almacenar todas las palabras generadas en el archivo word2.txt, para tener una idea con 5 palabras clave el comando generará un diccionario con **91975** palabras.

Ahora bien ya tenemos nuestro diccionario, podemos realizar un ataque con la herramienta SVCRACK para obtener contraseñas de las extensiones, la sintaxis es la siguiente:

svcrack –u(extension) (ip o dominio) –d (diccionario)

por ejemplo

svcrack –u101 192.168.1.50 –d word2.txt

Entonces el comando probara las palabras del diccionario en la extensión 101 de la central 192.168.1.50

Obteniendo el siguiente resultado:

Extension	Password
108	1234

FIGURA 7: RESULTADO SVCRACK

Ya tenemos la contraseña de una extensión podríamos configurarla en un softphone y empezar a realizar llamadas a través de ella.

Como hemos visto estos ataques han sido exitosos a nivel del dispositivo SIP encontrado, pero también podríamos escalar más en nuestros ataques, recordemos que el puerto 22 está abierto entonces usaremos la herramienta HYDRA para atacar este puerto. La sintaxis es la siguiente:

hydra –(opcion) –(diccionario) (ip o dominio) –(opciones adicionales)

por ejemplo

hydra –l root –P word2.txt 192.168.1.50 –t 8 –v ssh

Así indicamos que con el diccionario word2.txt encuentre la clave del usuario root, probando con 8 intentos a la vez.

El resultado obtenido es:

Host: 192.168.1.50 User: root Password: central2013

De esta manera nuestro ataque ha sido muy eficiente ya que tenemos acceso a la central como usuario root (todos los privilegios).

En este punto del proceso es alarmante la facilidad con la que hemos obtenido acceso a la central Elastix.

VI. PREVENIR ATAQUES

Como se ha mencionado anteriormente la finalidad de realizar hacking ético es encontrar vulnerabilidades de los sistemas, una vez encontradas es necesario buscar soluciones a las mismas.

En la siguiente figura se 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

FIGURA 8: VULNERABILIDADES ENCONTRADAS

Ahora veamos las soluciones a implementar:

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

FIGURA 9: SOLUCIONES A IMPLEMNTAR

VII. HERRAMIENTAS DE PROTECCIÓN

La plataforma de Elastix posee un módulo de seguridad que incluye un Firewall, este viene desactivado por defecto y la mayoría de usuarios no lo activan. Su uso es muy sencillo ya que posee una interfaz gráfica como vemos en la figura 10.

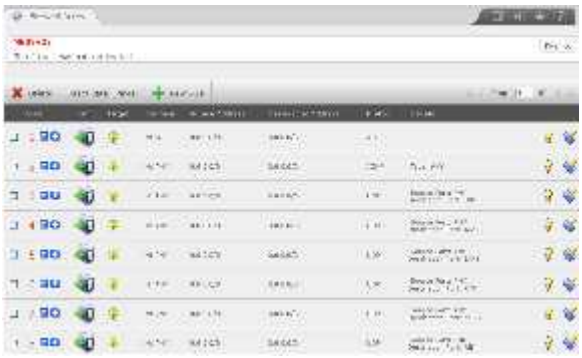

FIGURA 10: FIREWALL ELASTIX

Si configuramos esta herramienta de forma correcta evitaremos los accesos no autorizados, principalmente su utilidad es controlar los puertos y servicios en funcionamiento.

La plataforma también cuenta con la herramienta FAIL2BAN, la cual nos permite controlar los accesos concurrentes y por ende los ataques por fuerza bruta. De igual manera la herramienta viene instalada pero no configurada. Para configurarla existen varios tutoriales en internet.

Con estas dos herramientas configuradas, la implementación de contraseñas más robustas y la corrección del archivo sip.conf, nuestra central adquiere un nivel de seguridad bastante superior al que tenía previamente.

VIII. RESULTADOS FINALES

Después de implementar las solucione mencionadas volvemos a realizar las pruebas de penetración, los resultados son muy satisfactorios y se resumen en la siguiente tabla:

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

FIGURA 11: RESULTADOS FINALES

Para todos los casos vistos el resultado es exitoso, hemos conseguido prevenir ataques comunes en nuestra central Elastix.

IX. CONCLUSIONES

- El hacking ético es una herramienta útil y muy poderosa para prevenir ataques en nuestros sistemas y mejorar la seguridad de los mismos.
- La central Elastix posee varios puntos vulnerables si su instalación se realiza por defecto, sin configurar sus módulos de seguridad.
- Uno de los puntos más importantes a tomaren cuenta son las contraseñas débiles, aunque se configuren muchas herramientas de seguridad, éstas siguen siendo vulnerables si las contraseñas no son robustas.
- A pesar de obtener resultados exitosos después de implementar las soluciones propuestas, la central aún no está completamente segura, la única manera de garantizar su seguridad es innovar constantemente nuestras herramientas de prevención.

REFERENCIAS

- MATHEW, Thomas, Ethical Hacking and Countermeasures [EC-Council Exam 312-50] —Student Courseware, OSB Publisher © 2004.
- elastixtech.com/seguridad-básica-en-elastix/
- liberatech.mx/2013/04/configurar-fail2ban-en-elastix-2-4-paso-a-paso/

BIOGRAFÍA

Julio César Sotomayor Pozo, nació en Quito, Ecuador el 8 de mayo de 1987, Obtuvo el título de Bachiller en Físico Matemático en el colegio COTAC, sus estudios universitarios los realizó en la Escuela Politécnica del Ejercito en la facultad de Eléctrica y Electrónica.