PRUEBAS DE PENETRACIÓN EN SISTEMA DE TELEFONÍA IP EN SERVIDOR ELASTIX

Chaves García, Diego Andres.
dachga@gmail.com.
Bogotá, Colombia. Mayo 2016.
Universidad Piloto de Colombia.

***Resumen*—** Bien es conocido, que ante la vulnerabilidad de los sistemas de telefonía IP en servidor ELASTIX, los "delincuentes informáticos" incurren frecuentemente en este tipo de conducta delictual, al atacar los sistemas logrando provechos ilícitos; sin embargo, estos comportamientos es objetivamente previsibles y de solución técnica.
La razón:
Se presenta por no haberse realizado una protección adecuada, esto es, la debida implementación de VolP que este correctamente configurada, ya que esta inobservancia y/o su no incorporación, fácilmente conlleva y puede convertirse en un problema de seguridad para una organización, por cuanto permite a un "atacante "realizar llamadas con cargo a la factura de la compañía y demás consecuencias predecibles que esto genera, lo cual se traduce en un alto riesgo de pérdida económica.
Elastix es un sistema de comunicaciones unificadas de VolP que integra soluciones de fax, IMS, email y video. De manera nativa esta plataforma utiliza los protocolos SIP, IAX2, entre otros, que presentan múltiples vulnerabilidades. Con este artículo menciono los pasos básicos para realizar un ethical hacking, necesarios para llevar a cabo una prueba de penetración en una plataforma de VolP como elastix y, colocando de presente al revisar algunas de las vulnerabilidades conocidas del protocolo SIP.

***Abstract*—** While it is known that given the vulnerability of systems ELASTIX IP telephony server, "cybercriminals" frequently engage in this type of criminal behavior, attacking the making illicit profits systems; however, these behaviors is objectively foreseeable and technical solution.
The reason:
It is presented by adequate protection had not been made, that is, the proper implementation of VoIP that is properly configured, as this failure and / or non-incorporation, easily carries and can become a security problem for an organization, because allows an "attacker" calls charged to the bill of the company and other predictable consequences that this generates, which results in a high risk of economic loss.
Elastix is a unified communications system that integrates VoIP fax solutions, IMS, email and video. This platform natively uses the SIP, IAX2 protocols, among others, who have multiple vulnerabilities. With this article I mention the basic steps to perform ethical hacking, necessary to perform a penetration test on a platform VolP as elastix and placing of this to review some of the known vulnerabilities of SIP protocol.

I. INTRODUCCIÓN

En tratándose de sistemas de telefonía IP se han popularizado en las pequeñas y medianas empresas, permitiendo ahorrar costos reutilizando recursos actuales y minimizando cargos en los operadores. De ahí, que su despliegue sea rápido y fácil de implementar, lo que permite que las comunicaciones se efectúen unificadas en una sola plataforma; videoconferencias, llamadas también, mensajería instantánea, etc.
Ha de tenerse en cuenta, que conforme los registros de Cisco el tráfico cifrado de telefonía IP sobre internet ha aumentado hasta un 19% en el 2015[1], indicando el aumento de telefonía IP como un medio de comunicación óptimo y confirmando la preocupación de las organizaciones en mantener la seguridad en estas tecnologías.
Sostener unas condiciones cifradas no garantiza que los sistemas de VolP estén protegidos. Por eso como medida preventiva toda organización debe realizar pruebas de penetración a sus sistemas informativos.
Ante los hechos evidentes, que los "atacantes" estén desarrollando tecnologías y estrategias más sofisticadas, los cuales aumentan los riesgos para cualquier sistema informático, basta observar: *"Así mismo los delincuentes están creando infraestructuras y perfeccionando técnicas para quitarles dinero a las víctimas, robando datos y propiedad intelectual, evitando ser detectados"*[2]. Es de imperiosa necesidad la aplicabilidad del ethical hacking, el que entrega un valor agregado al permitir realizar una auditoría de cualquier sistema de seguridad, e identificar fallas de seguridad; para poder vulnerarlas y explorarlas, como lo haría un delincuente informático.
Ahora, con el ethical hacking se realiza una metodología la cual simula y crea un ambiente de prueba. Por tanto, hacer una intrusión a un sistema informático es la finalidad del ethical hacking; independiente del propósito o la intencionalidad del mismo.

II. SISTEMA DE VOIP

"Voz sobre Protocolo de Internet, también llamado voz sobre IP, voz 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

[1] http://www.cisco.com/c/dam/m/es_mx/offers/assets/pdfs/cisco_2016_asr_012816_es-xl.pdf, Pág.31
[2] http://www.cisco.com/c/dam/m/es_mx/offers/assets/pdfs/cisco_2016_asr_012816_es-xl.pdf, Pág. 2.

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. 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).
Es muy importante diferenciar entre voz sobre IP (VoIP) y telefonía sobre IP.
VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite comunicar voz sobre el protocolo IP.
Telefonía sobre IP es el servicio telefónico disponible al público, hace uso de la tecnología de VoIP"[3].

A. Componentes de la VoIP

Cliente: Es el origen de una llamada, genera la voz para que el dispositivo o teléfono, a través de un proceso de codificación convierta la señal analógica, en pulsos eléctricos y se pueda enviar por el medio de transmisión. Este cliente puede ser un teléfono convencional, un teléfono IP, un software que a través de un micrófono conectado a un computador realice una llamada por internet, etc.

Servidor: Se encarga del enrutamiento de llamadas, almacena una base de datos con registro de usuarios y de llamadas, también controla los servicios, la contabilidad y la recolección de las llamadas.

Gateways: Este provee las interfaces de comunicación con la telefonía tradicional y pueden ser interfaces FXO, FXS, E1s, etc. Adicionalmente es el puente de comunicación entre todos los usuarios, termina la llamada originada por el cliente.

Protocolos de VoIP: Son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

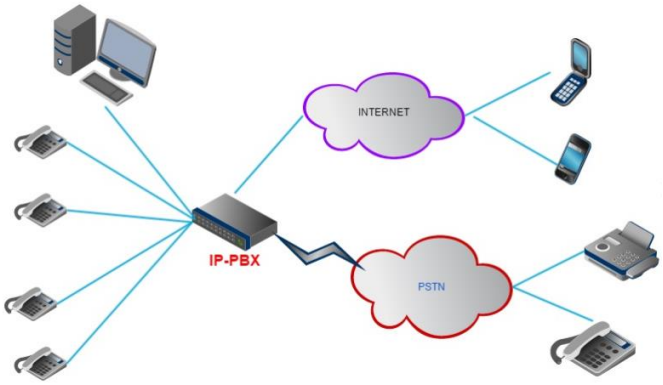

Figura 1. Central telefónica IP[4].

H.323 – Protocolo definido por la ITU-T; SIP – Protocolo definido por la IETF; Megaco (También conocido como H.248) y MGCP –protocolos de control; UNIStim – protocolo propiedad de Nortel(Avaya); Skinny Client Control Protocol – protocolo propiedad de Cisco; MiNet – Protocolo propiedad de Mitel; CorNet-IP – protocolo propiedad de Siemens; IAX – protocolo original para la comunicación entre PBXs Asterisk (Es un estándar para los demás sistemas de comunicaciones de datos, actualmente está en su versión 2, IAX2); Skype – protocolo propietario peer-to-peer utilizado en la aplicación Skype; IAX2 – Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX; Jingle – protocolo abierto utilizado en tecnología XMPP; MGCP- protocolo propietario de Cisco; weSIP- protocolo licencia gratuita de VozTelecom.

Codificación: Para transmitir la voz o el video por la red IP es necesario codificar y comprimir los datos, para luego ser decodificados y descomprimidos en el destino. Se utilizan una seria de Codecs que garantizan la codificación y los más utilizados en VoIP son G.711, G.723.1 y el G.729.

Anchos de banda para algunos codecs:
G.711: bit-rate de 56 o 64 Kbps.
G.722: bit-rate de 48, 56 o 64 Kbps.
G.723: bit-rate de 5,3 o 6,4 Kbps.
G.728: bit-rate de 16 Kbps.
G.729: bit-rate de 8 o 13 Kbps.

Las relaciones anteriores de ancho de banda para cada uno de los códec no es: *"el ancho de banda total utilizado, ya que hay que sumar el tráfico del códec, por ejemplo el Códec G729 utiliza 31.5 Kbps de ancho de banda en la transmisión"*5.

B. Funcionamiento básico

Un teléfono IP o un softphone en un computador, se encuentran conectados a la red LAN, se encargan de capturar la señal analógica de la voz y a través de un proceso de muestreo convierten la señal en pulsos digitales. Adicionalmente estos dispositivos convierten los pulsos digitales en paquetes IP, para enviarlos por la red LAN. Previamente el cliente se ha sincronizado en un servidor de telefonía IP o en una planta de telefonía IP.

Dependiendo del protocolo de comunicación que se esté utilizando (SIP, H323, MGCP, etc.) se enviarán los paquete de datos hacia diferentes puertos UDP, TCP o RTP. La voz se ha comprimido y codificado a través del Códec seleccionado. El servidor o planta realiza el puente para la comunicación con el receptor. Y el destino de la llamada puede ser una extensión local dentro de la organización, una llamada para una línea telefónica convencional, una llamada celular o hacia internet.

[3] http://elastixtech.com/fundamentos-de-telefonia/voip-telefonia-ip.
[4] Autor.
[5] http://elastixtech.com/fundamentos-de-telefonia/voip-telefonia-ip.

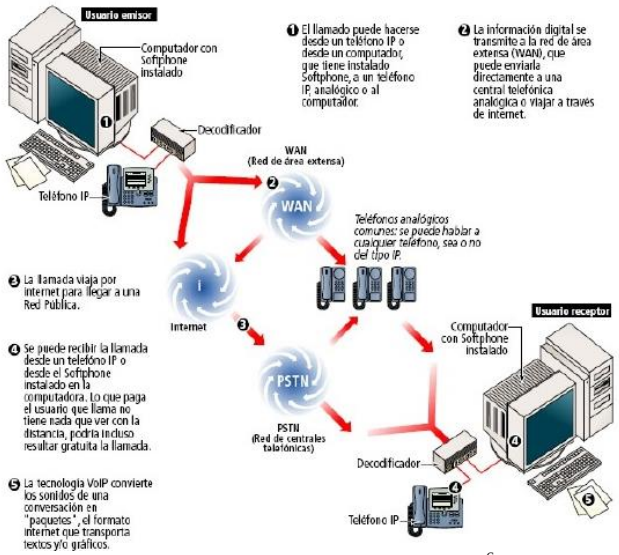

Figura 2. Funcionamiento de VoIP[6].

III. ETHICAL HACKING

Es una parte de la seguridad informática que utiliza una serie de herramientas, técnicas de ingeniería social, y exploits. Con el fin de explotar vulnerabilidades de los sistemas informáticos, para ello se utiliza una serie de ambientes de pruebas que simulan un ataque de un delincuente informático.

El objetivo del ethical hacking es poder revisar el nivel de seguridad de un sistema informático, incluyendo la seguridad física, las bases de datos, las aplicaciones, etc.

"A través del ethical hacking (es posible detectar el nivel de seguridad interno y externo de los sistemas de información de una organización, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica."[7]

Del ethical hacking salen dos términos el hacker y cracker. El primero accede a un sistema por conocimiento, por fines pedagógicos, por un contrato con una organización la cual requiere el nivel de seguridad en sus plataformas. A esta actividad se le conoce como hacking ethico y puede asimilarse a un auditor de seguridad de la información.

El cracker por el contrario es una persona malintencionada que desea sacar algún provecho del acceso no autorizado, como una remuneración económica, un robo de identidad, y todo tipo de acciones fraudulentas. En algunos casos son redes delincuenciales organizadas que realizan ciber-crimen y/o ciber-guerra.

El ethical hacking está dividido en dos partes, análisis de vulnerabilidades y pruebas de penetración.

Análisis de vulnerabilidades: Buscar vulnerabilidades del sistema que son conocidas, para identificarlas, clasificarlas y pueda determinarse la criticidad y el impacto al sistema informático.

Pruebas de penetración: Después de identificar las vulnerabilidades se intentan explotar de manera controlada, utilizando exploits conocidos o creando nuevos exploit.

[6]http://es.slideshare.net/danielayc/voip-315486/11.
[7]Tomado de http://www.seguridad.unam.mx/descarga.dsc?arch=2776.

Las pruebas de penetración se clasifican en:
Por el origen de las pruebas y por el conocimiento del objetivo.

Por el origen de las pruebas:

Externas: Son realizadas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad de la organización.

Internas: Son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad.

Por el conocimiento del objetivo:

Caja Negra: No se conoce nada del objetivo.

Caja gris: Se conoce muy poco del objetivo.

Caja Blanca: Se conoce mucho del objetivo.

A. Etapas del ethical Hacking.

Es la Metodología utilizada para realizar las pruebas de penetración y análisis de vulnerabilidades, las cuales están sustentadas en las normas y leyes como la circular 052, PCI DSS, ISO27001, OSSTMM, OWASP.

Las etapas son: Descubrimiento y enumeración, Análisis de vulnerabilidades, explotar vulnerabilidades, Reportar y recomendar.

1) Descubrimiento y enumeración.

En esta etapa se realiza una recolección de información, es conocer el contexto de la organización en donde se va a realizar la auditoria, esto incluye saber a qué se dedica y cuál es su misión.

El descubrimiento puede ser activo o pasivo.

Pasivo: Utilizar google hacking, operadores lógicos, para buscar bases de datos de archivos como Excel, Pdf y Word. Con esta información se puede realizar una ingeniería social enfocada al objetivo OSINT. En este paso, en ningún momento se debe generar un disparador en el objetivo, como activar un IDS o IPS, y la IP del auditor no puede ser piblicada. Se recomienda utilizar páginas como network-tools que brinden información como el sitio Web, Whois, escaneo de puertos, servidor de correo, etc. Siempre se debe proteger la IP e identidad del que realiza la recolección en este punto, tambien es importante hacer búsqueda inversa de imágenes.

Activo: En este parte realizamos un escaneo al objetivo, mostrando la IP del auditor, intentando recolectar un rango de direcciones IP, se puede revisar equipos activos, detectar DNS, sistemas operativos, encontrar firewalls, IPS e IDS, y también es posible la recolección de nombres de usuarios.

Se pueden utilizar varias herramientas, como dmitry, recon-ng, netdiscovery y la más completa es nmap. Esta aplicación realiza un escaneo profundo de puertos y servicios a través del ST (TCP Connect scanning) y Ss (Syn Scanning). El ST de nmap usa los sockets de Linux para conectar a la función connect () y simula una conexión como lo hace un computador. SS realiza una conexión TCP con el Three Way Handshake, aunque no se completa solo valida la recepción de un sync/ack y comprueba si un puerto se encuentra abierto o cerrado. El descubrimiento activo se conoce como enumeración.

2) Análisis de vulnerabilidades.

En esta etapa se realiza un modelado de infraestructura, servicios, aplicaciones, sistemas operativos e identificación de fallos conocidos (Infraestructura, servicios, apps y SO).

En base a la información recolectada en la fase previa, se puede determinar la ruta a seguir.

Se utiliza la información recopilada en la etapa de enumeración como las versiones, los servicios, los sistemas operativos y utilizamos herramientas que toman toda la información de la etapa de enumeración, y se compara con una base de datos de fallos de seguridad conocidos.

La información recolectada se puede organizar en una tabla, en escala de mayor a menor discriminando la criticidad de los fallos de seguridad, en los servicios y las aplicaciones.

Esta identificación de vulnerabilidades determinara la ruta a seguir, y se decide cual es el camino más acertado para poder llegar al objetivo.

En esta etapa es importante identificar si existe una metodología diseñada para el tipo de servicio, aplicación o infraestructura. Por ejemplo si se encuentra una infraestructura como una red inalámbrica existe la metodología OWISAM, si es una aplicación Web se utiliza la metodología OWASP. Y si no existe la metodología o no está definida se continúa a la siguiente etapa de explotar vulnerabilidades.

Metodologías open source disponibles:

- OSSTMM (Manual de Metodología Abierta de Evaluación de Seguridad).
- ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información).
- OWASP (Proyecto de Seguridad de Aplicaciones Web Abiertas).

Las vulnerabilidades se identifican a través de un diccionario común, este diccionario es público y es anunciado por la corporación Mitre, se conoce como (Common Vulnerability and Exposures) utiliza la sigla CVE.

Ejemplo de identificación:

CVE-1999-0003. Esta vulnerabilidad ejecuta comandos como root a través buffer overflow en un servidor de bases de datos tootalk.

Además las vulnerabilidades se clasifican a través del nivel de criticidad, y es definida por la NIST. Estas informan el nivel de impacto, tiempo, urgencia y prioridad en la solución de una vulnerabilidad. La clasificación se conoce como Common Vulnerability Scoring System, utiliza la sigla CVSS. Esta clasificación define un puntaje estandarizado, y es un marco de referencia el cual prioriza el riesgo.

El CVSS tiene la siguiente composición de métricas:

Grupo base: Identifica si la vulnerabilidad no cambia en el tiempo y el ambiente. AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C].

AV: Vector de acceso.

Au: Complejidad de acceso.

A: Autenticación.

Grupo temporal: Identifica si la vulnerabilidad cambia en el tiempo o la probabilidad de cuan explotable es la vulnerabilidad. E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]

E: Explotabilidad.

RL: Nivel de remediación.

RC: Confianza del informe.

Grupo ambiental: Identifica la influencia del entorno o el cálculo del riesgo en la estructura de una organización. CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND].

CDP: Daño colateral Potencial CDP.

TD: Distribución objetivo.

CR, IR, AR: Requerimientos de seguridad.

Algunas herramientas para realizar el análisis de vulnerabilidades:

Nessus, Retina community, Open vas, McAfee Vulnerability Manager, Qualys Guard.

3) *Explotar vulnerabilidades.*

En esta etapa el auditor simula los procedimientos y pasos que podría utilizar un hacker con malas intenciones, con el fin de explotar las vulnerabilidades encontradas. Aquí se dejan huellas del nivel de acceso alcanzado, y se recolectan todas las evidencias.

Se realizan ataques de fuerza bruta, crack de passwords, captura de tráfico en la red, se buscan y ejecutan exploits conocidos de los servicios encontrados, siempre dando prioridad a las vulnerabilidades más críticas según la clasificación de la NIST. Esta etapa es activa porque se deja al descubierto la IP del auditor, se disparan registros en los logs de los servidores, y se activan alarmas en los IDS o IPS.

En algunos casos se pueden intentar ataques de DoS, ingeniería inversa, realizar procesos de fuzzing, generar exploits, hacer escalamiento de privilegios, pivoting, y Dump. Es en este paso del ethical hacking, donde se recolecta toda la evidencia que se le va a entregar al cliente u organización, estas evidencias se entregan en un informe detallado.

Crack de passwords, parte esencial de esta etapa es intentar obtener contraseñas inseguras, para esto se utilizan diferentes técnicas para obtener las contraseñas, entre ellas se encuentran:

Fuerza Bruta, ataques de diccionario, tablas precomputadas, tablas arcoiris.

Fuerza Bruta: Probar todas las contraseñas posibles. Estadísticamente está comprobado que recorriendo el 50% de las posibles contraseñas se descubre la clave. Su efectividad está determinada por la longitud de la llave y el hardware requerido para hacerlo más rápido.

Ataques de diccionario: Se utiliza un diccionario o archivo con palabras conocidas en el idioma, combinando caracteres especiales, números, símbolos y la efectividad está determinada a la cantidad de palabras, calidad del diccionario, y la complejidad de la contraseña.

Tablas precomputadas: Es una tabla que contiene una palabra con su respectivo hash, y su funcionamiento está basado en la búsqueda del hash. La efectividad se determina por la cantidad de palabras en la tabla y normalmente una buena tabla precomputada puede pesar varios cientos de Gigabytes en almacenamiento.

Tablas Arcoiris: Esta técnica mejora el problema de espacio de las tablas precomputadas, se compara texto plano y hashes asociados a los textos, permitiendo obtener a partir de una operación lógica el hash para el texto plano y su respectivo password, en esta técnica se requieren maquinas con alta capacidad de procesamiento.

Existen Frameworks diseñados para explotar vulnerabilidades como metasploit, Coreimpact, Canvas y saint. El más utilizado es metasploit y es una herramienta opensource.

La aplicación corre una exploit conocido, permitiendo ejecutar un nivel de acceso a la vulnerabilidad encontrada. Cuenta con la mayor base de datos de exploits públicos y probados en la actualidad.

"Los pasos básicos a seguir para explotar las vulnerabilidades usando Metasploit son:

1. *Elegir y configurar el Exploit.*
2. *Opcionalmente confirmar si el objetivo es susceptible al exploit elegido.*
3. *Elegir y configurar el Payload (Código que se ejecutara una vez se explote la vulnerabilidad).*
4. *Elegir la técnica de codificación para que un IPS ignore el Payload.*

5. Ejectutar el Exploit.

Para poder elegir un exploit y un payload es necesario que contemos con alguna información del sistema remoto, tal como el Sistema operativo y servicios de red instalados."[8] Es importante aclarar que toda la información fue previamente recolectada en las etapas anteriores.

Pasos para realizar una prueba de penetración:

Identificar servicios y versiones, descargar exploit, revisarlo, lanzarlo, iniciar post-explotación.

4) Documentación

En esta etapa se presentan los resultados encontrados, se entregan preinformes, si se encontraron fallas criticas de seguridad o información que se considere importante o requiera mitigarse de manera inmediata. Los reportes deben ser ordenados, claros y completos. Tener presente el conocimiento del lector, no es lo mismo presentarlo para el administrador de seguridad, que para el director general de la organización. Por lo tanto se genera un informe técnico y otro informe ejecutivo.

Informe Técnico:

Dirigidos a los grupos de remediación, a los administradores de seguridad, líderes de proyectos, o analistas de TI. Se documenta a profundidad las pruebas realizadas y los hallazgos encontrados. Mostrar tablas, graficas de servicios críticos o vulnerabilidades críticas encontradas que permitan tomar decisiones inmediatas. Adicionalmente se detallan las herramientas a utilizar, se define el alcance del proyecto, las clausulas y legislación que aplique.

Este informe debe llevar los siguientes ítems:

Introducción, objetivos, alcance, Metodología, Resultados y conclusiones.

Informe Ejecutivo:

Dirigido a directores y ejecutivos, no se recomienda utilizar lenguaje técnico, debe ser compresible para personas que no tienen conocimiento en temas de seguridad informática.

El informe lleva los mismos ítems que el informe técnico pero se presentan resultados resumidos y ejecutivos. Se recomienda usar tablas estadísticas, números como cantidades de aplicaciones o equipos comprometidos y la cantidad de vulnerabilidades encontradas.

Lo más importante el impacto al negocio, si se encontró una falla de seguridad, se recomienda presentarlo en términos de riesgo y las consecuencias para la organización.

IV. PRUEBAS DE PENETRACIÓN SIP ELASTIX

Antes de realizar una prueba de penetración en una plataforma de VoIP, es necesario cubrir las siguientes etapas cuando se realiza la auditoria.

- Revisión de la infraestructura o arquitectura.
- Revisión de la seguridad en los servicios de voz publicados en Internet.
- Revisión de la seguridad de sistemas operativos, servicios de datos y aplicaciones.
- Analizar vulnerabilidades y determinar vectores de ataques.

A. "Metodología OSSTMM 2.1

1) Testeo de PBX.

Este es un método para lograr acceso privilegiado a la central telefónica de la organización objetivo.

- *Revisar los detalles de llamadas en busca de indicios de abuso.*
- *Asegurarse que las cuentas administrativas no tengan contraseñas por defecto, ni que las mismas puedan ser fácilmente adivinadas.*
- *Verificar que el sistema operativo se encuentre actualizado y con los últimos parches aplicados.*
- *Verificar el acceso remoto para el mantenimiento del sistema.*
- *Testear la autenticación de las llamadas entrantes.*
- *Verificar la autenticación remota de las llamadas entrantes.*

2) Testeo del correo de voz

- *Este es un método para lograr acceso privilegiado a los sistemas de correo de voz de la organización objetivo y de su personal interno.*
- *Verificar el tamaño del Pin y su frecuencia de cambio.*
- *Identificar información de usuarios y de la organización.*
- *Verificar el acceso remoto para el mantenimiento del sistema.*
- *Testear la autenticación de las llamadas entrantes.*
- *Verificar la autenticación remota de las llamadas entrantes.*

[8]Tomado de https://www.jsitech.com/linux/que-es-metasploit.

3) Revisión del Fax

Este es un método para enumerar máquinas de Fax y lograr acceso privilegiado a los sistemas en los que estos quizás se encuentren.

- *Asegurarse que las cuentas administrativas no tengan las contraseñas por defecto, ni que las mismas sean fácilmente adivinables.*

4) Testear Fax poling

- *Verificar el acceso remoto para el mantenimiento del sistema.*
- *Testear la autenticación de las llamadas entrantes.*
- *Verificar la autenticación remota de las llamadas entrantes.*

5) Testeo del Modem

Este es un método para enumerar módems y lograr acceso privilegiado a los sistemas de módems habilitados en los sistemas de la organización objetivo.

- *Escanear la central para módems.*
- *Asegurarse que las cuentas no tengan las contraseñas por defecto, ni que las mismas sean fácilmente adivinables.*
- *Asegurarse que el sistema operativo y las aplicaciones del modem estén actualizados y con los últimos parches aplicados.*
- *Verificar el acceso remoto para el mantenimiento del sistema.*
- *Testear la autenticación de las llamadas entrantes. Verificar la autenticación remota de las llamadas entrantes."*[9]

Modulo	Ciclos (días)	Degradación (%)	Influencia (x)
Revisión de Configuración de Seguridad	No Disponible	No Disponible	No Disponible
Revisión de la PBX	No Disponible	No Disponible	No Disponible
Testeo del Correo de Voz	No Disponible	No Disponible	No Disponible
Testeo del FAX	No Disponible	No Disponible	No Disponible
Inspección de Modems	No Disponible	No Disponible	No Disponible
Testeo de Controles de Acceso Remoto	No Disponible	No Disponible	No Disponible
Testeo de Voz sobre IP	No Disponible	No Disponible	No Disponible
Testeo de Red de Paquetes Conmutados X.25	No Disponible	No Disponible	No Disponible

Tabla 1. Valores de la Evaluación de Riesgo[10].

B. Procedimiento

1) Escaneo y monitoreo

En esta etapa el auditor recoge la mayor cantidad de información del sistema VoIP o la plataforma elastix.

Se utilizan herramientas como:

Nmap: obtener listado de puertos abiertos, sistema operativo.

SIPvicios: Obtiene un listado de cuentas de usuarios creados en un servidor Voip inseguro.

Shodan: Realiza descubrimiento de dispositivos como teléfonos IP.

2) Man in the middle

Capturar todo el flujo de llamadas, permite analizar el trafico SIP, RTP, IAX2.

Se utilizan herramientas como:

Wireshark: Analizador de tráfico de red permite capturar todo el tráfico de capa 2 en la red, se pueden capturar contraseñas y password de cuentas que podrían estar cifradas.

3) Romper contraseñas

Romper contraseñas de cuentas SIP, utilizando ataque de fuerza bruta, como john the riper, crear diccionarios, usar tablas precomputadas, y tablas arcoirirs para obtener el texto claro.

SIPcrack: Se intenta romper la contraseña de cuentas SIP usando una entrada estándar o con un diccionario.

SVCrack: Intenta romper las contraseñas de los registros del servidor VoIP, este ataque se realiza por fuerza bruta, permite realizarlo remotamente y depende de la latencia de la red.

Cain y Abel: Realiza ataques de fuerza bruta, utiliza diccionarios, tablas precomputadas, tablas arcoíris. Descifra los password capturados en la etapa de man in the middle.

4) Denegación de Servicio

Enviar una gran cantidad de volúmenes de paquetes de tamaños ajustados y deformes, evitando que el destino sea incapaz de proveer servicios. Incrementa ostensiblemente el consumo de CPU y el ancho de banda disponible.

Se utilizan herramientas como:

Udpflood: genera paquetes UDP 1400 bytes de tamaño como puerto destino el 5060 hacia el servidor Voip (Elastix).

Inviteflood: Genera paquetes invite al Servidor SIP, dirigida a una cuenta valida. Debido a que la mayoría de cuentas utilizan autenticación, el servidor responde a todas las peticiones intentando colapsarlo.

Rtpflood: Genera una gran cantidad de paquetes RTP. Previamente es necesario saber el puerto de escucha del objetivo.

Sipsak: Envía mensajes Options con el fin que el servidor responde con mensaje Ok. Se realizan muchas solicitudes colapsando el servidor.

5) Manipulación de Registro

En este paso se realiza manipulación de los registros, con el fin de sustituir un registro legítimo de una cuenta con una falsa que no existe.

Se utilizan herramientas como:

Reghijacker: Permite modificar los registros de un servidor Voip, en este ataque un usuario valido es sustituido por un usuario no registrado, toda la señalización entrante y saliente de comunicación del protocolo SIP, es dirigida al nuevo usuario creado.

6) SPIT (Spam Over Internet Telephony)

"VoIP está sujeto a su propio tipo de marketing no deseado, conocido como "Spam por telefonía de Internet" o SPIT"[11]. Se realizan llamadas a un extensión o cuenta del servidor, si la solicitud se responde se deja un mensaje de voz.

Herramientas disponibles:

SPITFILE: Fue desarrollado como herramienta de prueba para el rendimiento de un servidor SIP. Incluye una serie de escenarios básicos de usuario SipStone agente (UAC y UAS) y establece y libera múltiples llamadas con los métodos INVITE y BYE. Con esta tool se simula ataques de SPAM

[9]Tomado OSSTMM 2.1, Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM).

[10]Tomado OSSTMM 2.1, http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf Página 68.

[11] Tomado de http://co.norton.com/voip-security-a-primer/article.

SIP como objetivo un servidor Voip, consiste en inicializar una llamada y si el servidor responde, se deja un mensaje de alguna oferta comercial, intentando realizar una suplantación o vhishing.

7) Sistemas disponibles para realizar pentest a una plataforma de VOIP.

Actualmente en el mercado existen herramientas para realizar pruebas de penetración para algunos sistemas de VoIP.

- Metasploit módulo Voip. Version Free y Comercial.
- SPT System SIP.
- Viproxy MITM Proxy and Testing Tool.
- Viproy VoIP Penetration Testing and Exploitation Kit.

V. CONCLUSIONES

Conviene reiterar, al insistir en lo fundamental, como es el acogimiento de los sistemas de voz IP, y en especial Elastix; no solo por ser un servicio de bajo costo, sino también, por su despliegue de condición Open Source. Con lo cual, en algunos casos, al no ser necesario adquirir un hardware a algún fabricante, resulta obvio que disminuiría ostensiblemente los gastos, en razón a que se puede utilizar cualquier tipo de servidor compartiendo recursos como en una máquina virtual.

Ahora bien, los sistemas de VoIP ofrecen una gran cantidad de servicios unificados como es:

Conferencias, mensajería, video, fax, email y colaboraciones. Con lo cual se ahorrarían grandes costos a una organización u empresa.

Asimismo, teniendo en cuenta, cómo el crecimiento de las comunicaciones con VoIP se atribuye a sus evidentes beneficios, sin embargo muchos de sus protocolos de comunicación como SIP o IAX registran falencias que pueden ser explotadas. Con lo que se convierten en probable amenaza en el despliegue de esta infraestructura. Por tanto, tener estas vulnerabilidades sustenta la importancia de realizar un ethical hacking a la plataforma VoIP., siempre y cuando se dé cumplimiento a los siguientes requisitos:

Implementar una metodología adecuada, realizar todos los pasos necesarios para obtener la mayor cantidad de información del sistema auditado y, poder encontrar y documentar todos los hallazgos relevantes que podrían ser un riesgo económico o generar daño para el Core del negocio.

Como quiera que se conoce de la existencia de sistemas completos, que realizan las pruebas de penetración a cualquier sistema de VoIP como SPT System SIP, aunque su uso está restringido por el gobierno checo y es necesario realizar un registro que permita la identificación para poder usar dicha aplicación. Que mejor que buscar los beneficios al hacer uso de esta herramienta que propugno, la que bajo la perspectiva ofrecida se traduce en un sistema que tiene implementado módulos que realizan todos los pasos necesarios y mencionados en este artículo para realizar un pentest y que actualmente funciona como un servidor SIP de pruebas de penetración y puede realizar cualquier auditoria a servidores SIP locales o remotos.

Por último, como reflexión, si nos preguntamos: ¿A cuánto ascendería el quantum de pérdidas económicas por la incuria o impericia en la no aplicabilidad del ethical hacking a los sistemas? El solo imaginarnos la respuesta, genera preocupación su sumatoria que es gravísima, en razón a que en cualquier escenario empresarial generaría crisis y afectación económica. Por eso, a través de esta metodología o estrategia tecnológica su propósito transita y es todo un acierto preventivo, de ahí mi reiteración al reafirmarme que contribuye y se constituye en una verdadera garantía de solución al problema; que se debe acoger como protección, prevención y advertencia avizorando estar siempre adelantados a la intencionalidad dañina y perversa de los delincuentes cibernéticos.

REFERENCIAS

[1] Miroslav Voznak, Filip Rezac "Web-based IP telephony Penetration System Evaluating Level of Protection from Attacks and Threats" University of Ostrava Poruba, CZECH REPUBLIC, Noviembre 2011, pp 66-74.

[2] Gobel, Jan. Automatic Capturing of Malicious Software. Disponible: http://subs.emis.de/LNI/Proceedings/Proceedings170/177.pdf.

[3] Andres Mauricio, Mujica Zalamea, Hacking y aseguramiento de Servidores VOIP/SIP, *Presentación* XII Jornada Nacional de Seguridad Informática, Colombia, enero, 2012 Disponible: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/PresentacionAndresMujica-HackingServidoresVOIP.pdf.

[4] Gianluigi Me, Damiano Verdone, "An overview of some techniques to exploit VoIP over WLAN", University of Rome "Tor Vergata" Agosto, 2006, Pp 66-67.

[5] CERT Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP), Disponible: http://www.cert.org/advisories/CA-2003-06.html.

[6] H. Abdelnur, R. State, I. Chrisment, C. Popi. "Assessing the security of VoIP service", Villers-les-Nancy, France, 2007.

[7] Mitra, Alidoosti. Hassan, Asgharian. Ahmad, Akbari. "Security Framework for Designing SIP Scanner", Tehran, Iran, Marzo, 2013.

[8] Las vulnerabilidades VoIP, Norton Symantec, Disponible: http://mx.norton.com/voip-security-a-primer/article.

[9] Peter, Vincent Herzog, Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM), the Institute for Security and Open Methodologies, Agosto, 2003, Disponible: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf.

[10]Jasón, Soto, Que es metasploit, Abril, 2014, Disponible: https://www.jsitech.com/linux/que-es- metasploit.

[11] Daniela, Calva, Funcionamiento de sistema VoIP, Marzo, 2008, Disponible: http://es.slideshare.net/danielayc/voip-315486/11.

[12] Alejandro, Reyes, Galvy, Cruz, Andres, Hernandez, Equipo de Respuesta a Incidentes UNAM, Octubre, 2010. Disponible: http://www.seguridad.unam.mx/descarga.dsc?arch=2776.

[13] Fundamentos de Telefonía, Elastix Tech, Disponible: http://elastixtech.com.
[14]CISCO System, Reporte Anual de seguridad, Disponible: http://www.cisco.com/c/dam/m/es_mx/offers/assets/pdfs/cisco_2016_asr_012816_es-xl.pdf, Febrero, 2016.
[15] Introducción al pentesting, Dragonjar org, Medellín, 2014.

Autor

Diego Andres Chaves García.
Ingeniero Electrónico.
Universidad ECCI.
Bogotá, Colombia, 2010.
Seminario de Investigación Aplicada en Gestión del Riesgo, 2015.