Análisis y desarrollo de mejoras a un sistema honypot para mitigar ataques en servicios de VoIP

Analysis and development of improvements to a system honeypot to mitigate attacks on VoIP services

Juan Matías Koller[1], Mauricio Gabriel Bísaro[2]

Recibido: Abril 2015 Aceptado: Agosto 2015

Resumen.- La adopción por parte de empresas públicas y privadas de servicios de comunicaciones telefónicas sobre redes de datos IP, ya sea a través de la implementación de soluciones propietarias o de software libre, es un hecho en esta última década. Ahora bien, se sabe que sobre una red de datos que transporta servicios basados en IP existen muchas amenazas que pueden vulnerar y volver no disponible cualquier servicio. Para mitigar estas amenazas se requiere de un sistema de detección y control de ataques de firmas especializadas en el mercado de IT. Adquirir un producto de este tipo puede resultar inaccesible para muchas empresas, sobre todo para organismos públicos estatales, por su elevado costo. Debido a la importancia de contar con un sistema de detección de vulnerabilidades de costo razonable, es que se procedió a instalar y analizar la performance y operación del sistema honeypot[3] desarrollado en la Universidad Blas Pascal denominado "Artemisa[4]". Este sistema se instaló en la red de datos del gobierno de Córdoba para recolectar y analizar los ataques sufridos al servicio de telefonía IP. Después de clasificar y analizar los ataques, se añadió al sistema honeypot Artemisa la funcionalidad de interactuar con el firewall de perímetro del gobierno de Córdoba, proporcionando de esta manera un punto inmediato de defensa, permitiendo el bloqueo temprano e inmediato de los ataques del tipo flooding.

Palabras Clave: Honeypot; Flooding; Telefonía IP; Ataques; Seguridad informática.

Summary.- *The adoption of telephone communications over IP data networks by public and private companies, implemented either by means of proprietary solutions or by free software, it was a fact over the last decade as it is today. On the other hand, it is known that there are many threats in a data network carrying IP-based services that can infringe almost any service and make it not available. In order to mitigate these threats, an attack detection and control system it is required. Acquiring a product of this type can be unaffordable for many companies, especially for state government agencies as, in general, that kind of systems are too expensive. Therefore, because of the importance of having a vulnerability detection system at a reasonable cost, it was proceeded to install and analyze the performance and operation of a honeypot[3] system developed at Universidad Blas Pascal, called "Artemisa". Such*

1 *CIADE-IT, Universidad Blas Pascal, Córdoba, Argentina, matias_koller@yahoo.com.ar*
2 *CIADE-IT, Universidad Blas Pascal, Córdoba, Argentina, mbisaro@ubp.edu.ar*
3 *Herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas simulando ser vulnerable. https://www.projecthoneypot.org/*
4 *Software HoneyPot desarrollado en la Universidad Blas Pascal, http://artemisa.sourceforge.net/about.html*

a system was sniffing on the Córdoba State Government data network, for collecting and analyzing the attacks against IP telephony system. After some study and development, a feature for interacting with the perimetral firewall was added to the Artemisa honeypot system, providing an immediate point of defense, allowing the early and immediate blocking of flooding type attacks.

Key Words: *Honeypot; Flooding; IP telephony; Attacks; Computer security.*

1. Introducción.- Hoy por hoy, las empresas comienzan a emplear múltiples servicios de comunicaciones telefónicas basadas en el protocolo de internet (IP) sobre la infraestructura de la redes datos ya montadas. Esta adopción de las comunicaciones telefónicas empleando IP se hace en especial para amortizar el costo del alquiler o arrendamiento de los vínculos de datos, realizar un mejor aprovechamiento y utilización de los mismos, tener una mayor capacidad en el control de los gastos involucrados en las llamadas telefónicas, contar con una plataforma que integre las funciones de tarifación, gestión de llamadas, gestión de líneas, inventario del parque de línea telefónicas automática, entre las características que más se pueden destacar.

Las empresas en la actualidad pueden proyectar el despliegue de un esquema de telefonía IP corporativa gracias a la masificación de las redes de datos, su capilaridad para llegar a mayor cantidad de usuarios y la facilidad que poseen los usuarios de conectarse a internet, hacen posible que sean más los servicios que podamos ofrecer a los usuarios finales tanto en las redes privadas corporativas como en organismos de la administración pública provincial y nacional.

Si bien existen en el mercado tecnológico soluciones propietarias de telefónica IP, también existen soluciones de telefonía IP bastante más económicas que emplean software libre desarrollado bajo Linux. Las imágenes iso para la instalación de centrales telefónicas IP bajo linux son fácilmente accesibles en internet. Algunas de las distribuciones probadas y estables en el ámbito del gobierno de Córdoba son Elastix y Asterik[5].

Gracias a estas opciones de software libre, una empresa tiene la posibilidad de incursionar en el uso de servicios de telefonía IP y comenzar con la renovación de su red de comunicaciones telefónicas si cuenta con una red de datos IP.

Ahora bien, una empresa para implementar su propia red de telefonía IP además del hardware y software para establecer las llamadas, también necesita de equipamientos dotados con herramientas tecnológicas que permitan la protección de las comunicaciones entre los teléfonos y la central y la protección de las comunicaciones entre centrales. Estos dispositivos de protección deben permitir la detección de ataques, analizarlos y llevar a cabo las acciones de filtrado o bloqueo necesarias para mitigarlos, reguardando de esta forma la continuidad en la operación de las comunicaciones telefónicas.

En el mercado tecnológico existen soluciones propietarias de seguridad informática muy costosas, sobre todo para aquellas empresas que recién están incursionando en las comunicaciones telefónicas vía IP. Por este motivo, se procedió a la instalación, configuración, puesta en marcha y evaluación de desempeño de un sistema del tipo honeypot para la detección de ataques denominado Artemisa, desarrollado en la Universidad Blas Pascal. Este software esta implementado en lenguaje de programación python y fue concebido como un sistema de captura y registro de ataques únicamente [1]. Por consiguiente, no toma acciones contra el atacante mediante la interacción con dispositivos de seguridad informática como firewall o sistema de detección de intrusiones de una red datos.

5 *Son distribuciones de software libre para servidor de comunicaciones unificadas*

Se puede definir conceptualmente a un honeypot como un dispositivo que posee un software que simula ser un servicio particular, el cual está disponible para un fácil acceso para cualquier usuario dentro de la red de **datos [2]. A un** sistema honeypot se lo hace vulnerable y fácilmente accesible adrede. De esta manera se busca que los atacantes se vean seducidos a tratar de vulnerar su seguridad. Cuando esto ocurre, el honeypot registra los ataques que sufre y en función de ellos el administrador de seguridad informática puede actuar en consecuencia para mitigarlos.

La hipótesis que se plantea demostrar en el presente trabajo, es la gran utilidad y eficacia que posee el software honeypot Artemisa en la detección de ataques de flooding al protocolo SIP empleado para el inicio de sesión en las comunicaciones de telefonía IP [3]. Para demostrar su funcionalidad y eficacia se analizó su desempeño, funcionalidad y calidad de detección sobre una red de telefonía IP productiva de 2500 internos SIP. El otro aspecto a demostrar del sistema honeypot Artemisa, es la posibilidad de que el mismo pueda ser empleado como una alternativa a los sistemas de seguridad propietarios de firmas reconocidas de alto costo. Otro punto importante del análisis del sistema es hacer que el mismo pueda interactuar con el firewall de perímetro de la red de datos del gobierno de Córdoba para mitigar los ataques por flooding lejos de la ubicación física de las centrales telefónicas, para garantizar la continuidad de las comunicaciones telefónicas.

2. Ambiente de estudio.- Para demostrar las funcionalidades, la eficacia y precisión sobre el nivel de detección del software honeypot Artemisa, se llevó a cabo la instalación y configuración del mismo para que analice ataques al protocolo SIP dentro un sistema colaborativo de telefonía IP operando en la red de datos del gobierno de la provincia de Córdoba.

Como punto de partida antes de comenzar las capturas para su análisis, se instaló el sistema honeypot Artemisa sobre un servidor virtual con sistema operativo Linux Debian GNU [4]. El honeypot Artemisa simula ser un teléfono IP a nivel de software, registrado como un teléfono válido sobre una central telefónica IP de marca Philips [1]. De esta forma siendo parte del plan de discado de la central telefónica, éste recibe indirectamente ataques de flooding dirigidos a ésta. En esta infraestructura de prueba el honeypot cumple el papel de un teléfono SIP estándar. Vale destacar que se analizaron únicamente los ataques sufridos a dispositivos configurados como internos de esta central, ya que es la que más volumen de internos SIP tiene y además es la central gateway hacia la red de telefonía pública (PSTN) para el resto de las centrales indicadas en la figura I.

Por tratarse el sistema Artemisa de un honeypot, es indispensable que esté accesible para los atacantes sobre la misma subred IP de operación que la central a analizar. Es necesaria esta forma de conexión, ya que muchos de los ataques se originan con tráfico de difusión a nivel capa enlace de datos del modelo de referencia TCP/IP, en especial los ataques de flooding. Los ataques de este tipo emplean la dirección MAC de destino de difusión con el valor FF-FF-FF-FF-FF-FF. La dirección MAC es un campo que es parte de la trama del protocolo Ethernet empleado en la capa enlace de datos por las redes de datos actuales. Toda trama que emplee esta dirección de difusión como destino, hace que ésta llegue a todos los dispositivos IP de la red de datos. Si el honeypot y la central telefónica a analizar se encuentran en distintas subredes IP, los enrutadores no permiten el traspaso de trafico de difusión a nivel MAC Addresss, lo que lleva a que el honeypot no detecte el tráfico de flooding capa 2.

En la figura I se observa el esquema de conexión del sistema honeypot Artemisa para registrar los ataques que sufre la central Philips. En la Tabla I se muestran las capacidades de internos que presenta la central analizada. Tanto la figura I como la tabla I, reflejan lógicamente la envergadura y capilaridad de la red de telefonía IP a analizar.

Central Philips – Sistema Operativo IS 3000 – Version 4.1				
Cantidad de Internos Digitales	Cantidad de Internos Analogicos	Interno Sip	Tramas E1	Lineas Analogicas R2
200	405	2500	4	20

Tabla I.- Composición de las centrales telefónicas empleadas para el análisis

Para determinar el grado de eficacia en la detección que posee el sistema honeypot Artemisa, se emplearon herramientas que se adoptaron para generar y forzar ataques dirigidos hacia éste. Estas herramientas se emplean comúnmente sobre redes de datos IP para la realización de pruebas de penetración y verificación de seguridad de diferentes servicios. Entre las herramientas de pruebas de seguridad empleadas se destacan [5]: kali, vast viper, SIPVicius, SipDump, inviteflooding Sipp, Sipsak, PROTOS y Spitter[6].

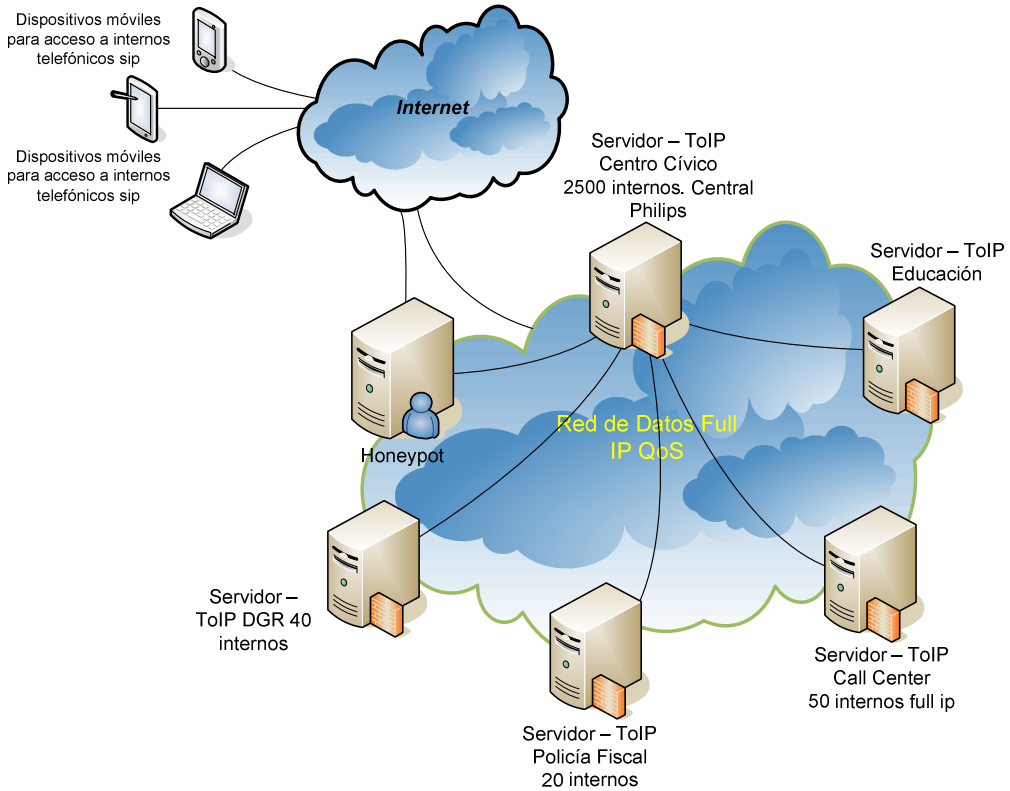

Figura I.- Esquema lógico de operación del honeypot

En la figura I, se observa como el sistema honeypot Artemisa se registra como un interno sip de la central Philips. De esta manera se enlazo al sistema honeypot Artemisa al esquema de numeración de internos sip de la central Philips. Las siguientes extensiones se configuraron en cada dispositivo.

6 *Herramientas de generación de ataques a infraestructuras de telefonía IP. http://www.hackingvoip.com/sec_tools.html/*

ISSN 2301-1092 • ISSN (en línea) 2301-1106

Configuración de Internos en el sistema honeypot Artemisa			
Direccion IP del Servidor sip en central Philips	Numero de interno sip	Nombre de usuario sip	Password de registro sip
10.48.250.232	3767	3767	3767
10.48.250.232	3768	3768	3768

Tabla II.- Configuración honeypot

Si bien el esquema de telefonía IP que presenta la figura I es complejo en cuanto a cantidad de centrales, se optó únicamente por informar los ataques sufridos por dispositivos conectados a la central Philips que es la que mayor cantidad de internos presenta. Para futuros análisis de ataques hacia otras centrales, el procedimiento de instalación, configuración y puesta en marcha del sistema honeypot Artemisa es idéntico al mostrado en el presente trabajo: se define un servidor virtual nuevo, se instala el sistema operativo, se instala el software Artemisa, se conecta el servidor a la misma subred de la central a analizar, se lo registra en la central para que sea parte de su plan de internos y comenzará a capturar y a mitigar ataques automáticamente. Es importante destacar que se pueden configurar varios internos sip de distintas centrales en el sistema honeypot, solo hay que tener en cuenta la sobrecarga o el consumo excesivo que esto puede provocarle.

3. Configuración del HoneyPot.- A continuación se muestra cómo se realizó la configuración del Honeypot para el análisis de los ataques en la red. Como se muestra en la tabla II, el honeypot se registra como un interno de la central Philips para comenzar con la captura. Se le definió al sistema honeypot una dirección IP dentro de la misma subred que la central Philips. La instalación del honeypot se realizó en un servidor Dual Core de 2,5 GHz, 8 GB de RAM sobre el sistema operativo Linux Kali[7] y se alojó en el directorio /home/ artemisa_1.0.91.

En el directorio /conf del sistema honeypot Artemisa, se encuentran los archivos de configuración donde se definen la dirección IP de la central a analizar y la dirección de IP de las extensiones, las acciones a tomar y el comportamiento que tendrá el honeypot. Los archivos de configuración que se muestran a continuación son los pertenecientes al honeypot asociado a la central Philips.

```
root@kali:/home/artemisa_1.0.91/conf#ls
total
actions.conf
artemisa.conf
behaviour.conf
extensions.conf
servers.conf
```

Figura II.- Archivos de configuración del sistema honeypot

7 *Distribución basada en Debian GNU/**Linux** diseñada principalmente para la auditoría y seguridad informática en general*

6

En el archivo artemisa.conf, tiene lugar la configuración principal del sistema honeypot. Aquí describiremos las líneas principales de configuración. Las referencias indicadas en cada una de las figuras mostradas a continuación al lado de cada línea con el símbolo **->,** muestran la función de cada opción de configuración.

```
#
[environment]
local_ip=10.48.250.240          -> Dirección de IP del Honeypot
local_port=5060                 -> Puerto de Servicio
sip_domain=10.48.250.232        -> Dirección de IP de Central a asociar
user_agent=Twinkle/1.4.2        -> Tipo de dispositivo o agente back-end
playfile=sample.wav             -> Archivo de Audio
behaviour_mode=active           -> Comportamiento o acciones que tomara el HPot
max_calls=1                     -> Llamadas máximas a atender
#fingerprint_mode=passive       NOT YET IMPLEMENTED
# [sound]
[sound]
enabled=true                    -> Deshabilita la grabación de Media
device=0
rate=44100
```

Figura IV.- Figura III - Archivo de configuración principal de honeypot

Los siguientes archivos de configuración se son empleados para definir el servidor de comunicaciones vía IP (en este caso la central Philips) y las extensiones de la misma utilizada para el análisis de ataques sobre la citada central.

```
# Artemisa - Servers configuration file
[Philips]
registrar_ip=10.48.250.232      -> IP donde se registra el Honeypot
registrar_port=5060             -> Puerto de registración
registrar_time=3600             -> tiempo de duración
nat_keepalive_interval=30
exten=3767,3768                 -> Extensiones a registrar

# Artemisa - Extensions configuration file
[3767]                  -       > Numero de extensión de la central
username="3767"
password=3767

[3768]
username="3768"
password=3768
```

Figura IV.- Archivo de configuración server.conf

Sobre el archivo de configuración actions.conf se asignaran los campos de información a registrar en cada acción detectada flood, spit o scan. Para este análisis y posterior evaluación se emplearan los valores por defecto. Por último en el archivo behaviour.conf se define el comportamiento que tendrá el sistema honeypot Artemisa: pasivo, activo o agresivo.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

4. Implementando los ataques.- Para realizar la prueba de desempeño del sistema honeypot Artemisa, determinar su grado de precisión en la detección de los ataques y en función de lo detectado aplicar las mejoras al mismo, se emplearan herramientas de seguridad informática utilizadas para pruebas de penetración y detección de vulnerabilidades. Los tipos de firmas y ataques que detecta el sistema honeypot Artemisa, están indicados en el archivo fingerprint.txt, detalladas a continuación:

- PROTOS Test-Suit (c07-sip): a SIP Torture Test that allows sending a major amount of malformed messages:
- Sipscan : supports REGISTER, OPTIONS and INVITE scanning;
- SIPVicious: enumerates SIP servers in a given IP range by sending OPTIONS or INVITE messages;
- Inviteflood : simple tool that allows several types of flooding based attacks;
- Sipp: allows testing the SIP servers performances under stress conditions;
- Sipsak: command-line SIP testing tool helpful for flooding and robustness tests;
- Spitter: works over Asterisk and automatically generates calls with an audio message to be delivered;
- SIP Send Fun13: supports several fuzzy INVITE messages for robustness testing;
- SipBot14: remotely controlled SIP attack tool supporting several attack commands.
- VoIPER15: es un conjunto de herramientas para realizar fuzzing y torturing.

Para empezar a observar comportamiento en el sistema hemos forzado, en algunos casos, ataques contra la central y el dispositivo honeypot. En este punto se activó el honeypot, dejándolo en funcionamiento para determinar si lograba detectar los ataques realizados.

El archivo fingerprint.txt contiene las firmas y patrones que el sistema honeypot detecta, este archivo se encuentra alojado en /../../. El sistema permite agregar nuevas firmas y patrones de ataques incluyéndolos en este archivo, de esta forma se puede aumentar la cantidad y tipos de herramientas a detectar, mejorando la capacidad de detección del honeypot.

A continuación aplicaremos las herramientas de penetración a la seguridad informática para probar el desempeño y eficacia de detección del sistema honeypot Artemisa.

4.1. Escaneo de internos - El primer paso tomado para las pruebas de operación del sistema honeypot, fue realizar un descubrimiento de la red interna en busca de dispositivos que utilicen el protocolo SIP. Para ello se utilizó la herramienta de seguridad a nivel de software svmap, una herramienta de la suite de SIPvicious.

```
root@kali:~# svmap -p5060-5062 10.48.250.0/24  -m INVITE
```

Para la prueba se definieron opciones especificando un rango de puertos para la red a escanear. También se utilizaron escaneos con el campo OPTION y REGISTER. Los dispositivos encontrados fueron los descritos a en la figura VI.

SIP Device	User Agent	Fingerprint
10.48.250.240:5060	Twinkle/1.4.2	disabled
10.48.250.111:5060	iS3000 SIP Server 8851.01.0.0	disabled
10.48.250.232:5060	iS3000 SIP Server 8851.02.0.0	disabled
10.48.250.234:5060	friendly-scanner	disabled
10.48.250.101:5060	iS3000 SIP Server 8851.01.0.0	disabled

Figura VI.- Dispositivos SIP encontrados mediante herramienta de escaneo.

El resultado arrojado por el sistema honeypot Artemisa en respuesta a la acción de ataque generada por la herramienta svmap se muestra en la figura VII. Solo se coloca un extracto de la salida del sistema Artemisa, el más relevante, que indica el tipo de análisis realizado.

```
Artemisa's report
********************************************************************************
**********
Results
********** Information about the call**********************

From: 3568838573 in 10.48.250.240:5060/udp
To: 3568838573 in 10.48.250.240
Contact: 3568838573 in 10.48.250.240:5060/udp
Connection:
Owner:
Via 0: 10.250.6.243:5060/udp
User-Agent: friendly-scanner
Artemisa concludes that the arrived message is likely to be:

* The attack was created employing the tool SIPVicious.
* A scanning attempt.
* The message belongs to a ringing attack.
```

Figura VII.- Reporte del sistema honeypot

En la figura VII se muestra que el resultado de la detección del honeypot fue acertado, indicando que la herramienta utilizada fue svwar de la suite SipVicious.

A continuación se realizó un escaneo de internos de la central Philips con la herramienta de seguridad “svwar” en un rango de 1000 internos. Como resultado de la prueba se pudo recabar información de los internos de la central (solo se colocaron los internos más significativos a modo de muestra, ya que el reporte sin restricción muestra los 2500 internos operativos).

ISSN 2301-1092 • ISSN (en línea) 2301-1106

```
root@kali:~# svwar -e3000-4000 10.48.250.232
| Extension | Authentication |
------------------------------
| 3190      | reqauth        |
| 3810      | reqauth        |
| 3799      | reqauth        |
| 3109      | reqauth        |
```

También probamos contra el honeypot, solo para observar su reacción.

```
root@kali:~# svwar -e3000-4000 10.48.250.240
WARNING:root:found nothing
```

Como resultado de estas dos acciones el honeypot solo mostro información sobre los ataques realizados a él directamente y no hubo detección sobre el tráfico atacante al resto de los internos de la central. El tráfico atacante es analizado solo si llega a su interfaz. También se puede ver que al no tener un dial plan configurado el Honeypot no devuelve resultado alguno.

A continuación vemos el resultado desplegado por el sistema honeypot Artemisa ante la búsqueda de información de extensiones tanto en la central Philips como en el honeypot. Este tipo de ataque fue el más reiterado en la red de telefonía IP del gobierno de Córdoba.

```
Artemisa's report
**********************************************************************
**********
Results
**********************************************************************
**********
********** Information about the call
**********

From: 3003 in 10.48.250.240:5060/udp
To: 3003 in 10.48.250.240
Contact: 3003 in 10.48.250.240:5060/udp
Connection:
Owner:
Via 0: 10.250.6.243:5060/udp
User-Agent: friendly-scanner

Artemisa concludes that the arrived message is likely to be:

* The attack was created employing the tool SIPVicious.
* Dial plan Fault
```

Figura VIII.- Comportamiento y detección generado por el honeypot

4.2. Ataques por Flooding.- En esta sección se prueba el funcionamiento del sistema honeypot Artemisa y su respuesta ante un ataque de inundación contra la central Philips. Esta ataque

consiste en enviar múltiples INVITE de inicio de sesión a internos de una central IP para que esta los dirija hacia los dispositivos y de esta forma provocar un ringing masivo de los teléfonos IP. Con este ataque se intenta colapsar la operación de la central y entorpecer el funcionamiento del servicio. Para generar el ataque se utiliza una herramienta de flooding para el protocolo SIP conocida como inviteflood.

```
root@kali:~# /usr/bin/inviteflood eth0 376771 10.48.250.232 10.48.250.232 10000

inviteflood - Version 2.0
        June 09, 2006

source IPv4 addr:port   = 10.250.6.243:9
dest   IPv4 addr:port   = 10.48.250.232:5060
targeted UA             = 3171@10.48.250.232

Flooding destination with 10000 packets
sent: 10000
```

Figura X.- Implementación de herramienta de ataque por flooding

En la figura X se realiza un ataque de inundación a la central utilizando uno de los internos obtenidos mediante el escaneo de extensiones a la central. En este caso se usó el interno 3767, que es una extensión asignada al dispositivo honeypot. También podría realizarse el ataque a un rango de internos, si no se conocen estos previamente y de estar incluido el interno del honeypot en el ataque se obtendrá el mismo resultado como se muestra en la figura XI.

La información obtenida por el honeypot fue acertada en cuanto a la herramienta utilizada y al tipo de acción tomada contra el dispositivo, lo que se muestra en la figura XI.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

```
Artemisa's report
********************************************************************************
**********
Results
********************************************************************************
**********
********************************** Information about the call
**********************************

From:  in 10.250.6.243:9/udp
To: koller in 10.48.250.232
Contact:  in 10.250.6.243:9/udp
Connection: 10.250.6.243
Owner: 10.250.6.243
Via 0: 10.250.6.243:9/udp
User-Agent: Elite 1.0 Brcm Callctrl/1.5.1.0 MxSF/v.3.2.6.26

Artemisa concludes that the arrived message is likely to be:

* The attack was created employing the tool inviteflood.
* A flooding attack.
```

Figura XI.- Información y detección de la herramienta de ataque por flooding

4.3. Ataques por escaneo.- Otra herramienta empleada para las pruebas de desempeño del sistema honeypot Artemisa fue Sipp. Esta herramienta permite realizar un escaneo de puertos activos en las centrales telefónicas que emplean SIP como protocolo de inicio de sesión. A continuación se muestran los resultados obtenidos de las pruebas realizadas a la central Philips.

```
root@kali:~# sipp 10.48.250.240 -sn uas
Warning: open file limit > FD_SETSIZE; limiting max. # of open files to FD_SETSIZE = 1024
      Resolving remote host '10.48.250.240'... Done.
---------------------------- Scenario Screen -------- [1-9]: Change Screen --
 Port   Total-time  Total-calls  Transport
 5060      2.93 s          1  UDP
 0 new calls during 0.929 s period     1 ms scheduler resolution
 1 calls                       Peak was 1 calls, after 0 s
 0 Running, 3 Paused, 3 Woken up
 0 dead call msg (discarded)
 3 open sockets
                      Messages  Retrans   Timeout   Unexpected-Msg
          ----------> INVITE          1           0          0
           <---------- 180                  1         0
          <---------- 200                  1         0          0
          ----------> ACK        E-RTD1          1          0
           ----------> BYE                 0          0          0
          <---------- 200                  0         0
          [   4000ms] Pause                0                    0
```

Artemisa's report

****
****
Results
****
****
********** ***Information about the call***
****
From: sipp in 127.0.1.1:5060/udp
To: service in 10.48.250.240
Contact: sipp in 127.0.1.1:5060/udp
Connection: 127.0.1.1
Owner: 127.0.1.1
Via 0: 127.0.1.1:5060/udp

********** ***Classification***
****
+ Checking fingerprint...
| Fingerprint found. The following attack tool was employed: Sipp
| Category: Attack tool
+ The message is classified as:
| Attack tool
| Spoofed message
| Dial plan fault
| Scanning
| Ringing

********** ***Correlation***
****
Artemisa concludes that the arrived message is likely to be:

**** The attack was created employing the tool Sipp.***
**** A scanning attempt.***

Figura XII.- Técnica de ataque y respuesta del honeypot

Como puede apreciarse en la figura XII, el sistema honeypot detecta correctamente la herramienta de software empleada denominada Sipp y el tipo de ataque realizado con la misma. Se comprobó que el Honeypot detecto la herramienta SipScan la cual es empleada para realizar inundación de tráfico (flooding). El reporte con los resultados obtenidos por el sistema Artemisa puede verse en la figura XIII.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

Artemisa's report
****
****
Results
****
****
********** ***Information about the call***
****
From: test in 464982:5060/udp
To: in 169.254.85.7
Contact: test in :5060/udp
Connection: 169.254.85.7
Owner: 169.254.85.7

Via 0: 169.254.85.7:62794/udp
User-Agent: X-Lite release 1105x

********** ***Correlation***
****
Artemisa concludes that the arrived message is likely to be:

**** The attack was created employing the tool SIPSCAN.***
**** A scanning attempt.***

Figura XIII.– Resultado ante una variante en la herramienta

También se han observado intentos de flooding mediante los campos REGISTER y OPTIONS. Estos han sido detectados correctamente por el sistema Honeypot y mostrados por pantalla, pero no dejan registros en el archivo de log del dispositivo.

5. Mejoras adoptadas en el sistema Honeypot.- Una vez recolectados los datos de los ataques, ya sea naturales o forzados con las herramientas indicadas en la sección 4, se pudo determinar que la mayoría de los ataques recibidos por la central Philips del gobierno de Córdoba fueron intentos de flooding. Por este motivo, se decidió agregar una mejora en la operación del sistema honeypot Artemisa. Para ello se aplicó una acción de bloqueo en el script de flooding, basándose en la dirección IP de origen del dispositivo atacante, dato que se encuentra en los reportes del sistema honeypot Artemisa.

De esta manera se configuro una acción dentro del script on_flood.sh para que inserte en un firewall (de la marca FORTINET®) la dirección del atacante y la asigne a un grupo de bloqueo, que luego se agregó a una política de firewall [6].

Cabe destacar, que el sistema honeypot interactúa con un firewall de la marca Fortinet, porque es el equipo de seguridad perimetral por donde pasa todo el tráfico de la red de datos. En consecuencia, realizando el bloqueo en este dispositivo de cualquier tráfico malicioso evitamos que ese tráfico pase hacia su destino de ataque.

La operación del bloqueo funciona de la siguiente manera: Una vez que el Honeypot detecta la acción de flooding llama al script on_flood.sh en el directorio /scripts. En este script se introdujo el código que se muestra en la figura XIV.

```
#!/bin/bash

# This script is executed when flooding is detected. It may be used to activate some firewall rule
and avoid a DoS attack.

#You can use this to set a rule in iptables and block the attacker
echo "================================\n"
echo ">>" $1 "<<"                                -> Mostramos la IP
echo \n
echo "================================"
/home/artemisa_1.0.91/scripts/forti $1        → Llamamos al script llamado forti y mandamos la IP
como parámetro
/home/artemisa_1.0.91/scripts/forti $1 | /usr/bin/sshpass -p 123456 ssh prueba@10.225.26.254
# Luego lo enviamos al firewall conectándonos a este por medio de ssh con el usuario prueba y la
password 123456

echo "block ip executed done"
echo "================================"

El script denominado forti consta de la siguiente estructura y sirve para agregar la dirección en el
equipo y asignarla al grupo de bloqueo.

#!/bin/sh
echo "config firewall address"                   → Ingresa al modo de configuración del
objeto
echo "edit IP_BLOQUEADA"                         → Crea el objeto que contendra la Dir. IP
echo "set associated-interface \"internal\""     → Asocia el objeto a la interfaz de entrada
echo "set subnet $1 255.255.255.255"             → Setea la dirección de red
echo "next"
echo "end"

echo  "config firewall addrgrp"                  → Ingresa al modo de configuración del
grupo
   edit "G_IP_FLOOD"                             → Edita el grupo de bloqueo
        set member "IP_BLOQUEADA"                → Agrega la ip al grupo de bloqueo
   next
end
```

Figura XIV.– Código del Script para bloqueo temporal ante un ataque de flooding

Es importante destacar que para poder insertar en el equipo firewall Fortinet9[8] la dirección IP a bloquear se debe crear previamente un usuario y una clave, el grupo de bloqueo y la regla de acceso en éste. En el firewall se deberá denegar el acceso al grupo de bloqueo.

6. Conclusiones.- Después de realizado el análisis de desempeño del sistema honeypot Artemisa se ha podido corroborar que el mismo es apto para la detección de escaneos de red en busca de dispositivos sip, intentos de búsqueda de dial plan e intentos de saturación para lograr denegación de servicio en la central analizada a través de tráfico de flooding. Dentro de los análisis del tipo

8 *http://www.fortinet.com/resource_center/whitepapers.html*

ISSN 2301-1092 • ISSN (en línea) 2301-1106

flooding se pudo determinar que el sistema honeypot detecta y registra los ataques mediante INVITE. En cambio, el sistema honeypot solamente detecta pero no registra los ataques de intentos de flooding empleando el campo REGISTER u OPTIONS. Es necesario que los ataques queden registrados en el script correspondiente, porque a partir de esta información se interactúa con el firewall.

El sistema honeypot Artemisa demostró una operación estable ante ataques de flooding no llegando a quedar indisponible en su funcionalidad por falta de recursos de harware: cpu y ram. El sistema honeypot es parametrizable en cuanto a la cantidad máxima de sesiones a analizar, otro punto fuerte que permite resguardar los recursos de cpu y ram del servidor donde se ejecuta el sistema honeypot. El sistema permite añadir nuevos patrones o firmas de ataques en el archivo fingerprint.txt, lo que lo hace escalable ante la aparición de nuevos software maliciosos.

La operación del sistema honeypot Artemisa en la red de telefonía IP del gobierno de Córdoba, demostró ser lo suficientemente óptima y confiable, lo que permite sentar precedentes para que muchas empresas públicas y privadas evalúen la posibilidad de adoptar este sistema de detección en su propia red de telefonía IP.

Los resultados obtenidos durante los 6 meses de operación del sistema honeypot Artemisa con ataques forzados y naturales dentro de la red de datos del gobierno de Córdoba, arrojaron que la herramienta es apta y confiable con un nivel de detección del 98% en cuanto a ataques de SIP flooding y escaneos de internos (dial plan). En la figura siguiente se muestran los resultados de la operación del sistema honeypot.

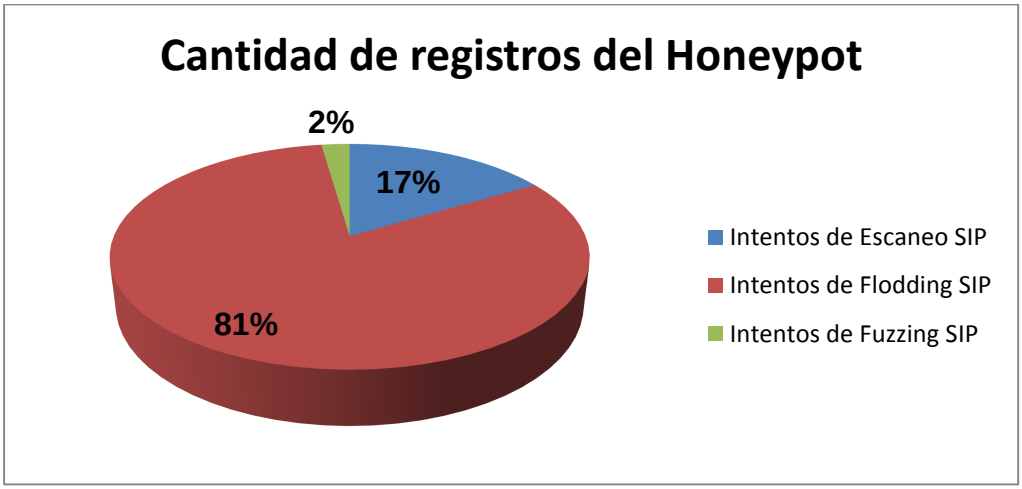

Figura XV.- Estadísticas de ataques detectados por el honeypot dentro de un ambiente productivo

Del resultado de las pruebas, se pudo diseñar y programar una mejora importante en el sistema honeypot. Esta mejora consistió en la creación de un script integrado el sistema honeypot para proporcionarle a la organización un punto inmediato de defensa. Este script permite que el sistema honeypot interactué con el firewall de perímetro que posee el gobierno de Córdoba, permitiendo de esta manera el bloqueo temprano y el corte ante ataques de flooding.

Gracias a la escalabilidad del sistema honeypot Artemisa es que en la actualidad se está desarrollando un módulo que mitigue los ataques en el punto de conexión directo del atacante. De esta manera se aislará al atacante de forma inmediata sin que el tráfico malicioso se

introduzca profundamente en la red de datos (pasando de la red de acceso al core). Esto es necesario ya que todo ataque genera consumo de recursos en la red de datos, como ser: memoria y uso de cpu de los switches y routers intermedios. El desarrollo incluye la interacción a través del protocolo de gestión de red simple (SNMP) y las Bases de Información de Gestión (MIBs) de los switches con el sistema honeypot Artemisa. La mejora en desarrollo apunta a trabajar en una ambiente LAN controlado, donde se conoce la topología de la red y el honeypot permita cargar las MIB de los equipos configurable. Estas nuevas mejoras apuntan a reforzar lo expuesto en el presente trabajo, para que las empresas tengan la opción de evaluar y emplear un software libre de control de ataques de bajo costo como alternativa a los costosos equipos y herramientas dedicadas a la seguridad informática.

7. Referencias

[1] Do Carmo, R.,Masri, Diseño de un honeypot para mejorar la seguridad en la red de telefonía IP del gobierno de la provincia de Córdoba, U.B.P., 2009.

[2] M. Nassar, R. State and O. Festor, "VoIP Honeypot Architecture," in Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on, vol., no., pp.109-118, May 21 2007-Yearly 25 2007

[3] J. Rosenberg, et al., *SIP: session initiation protocol. RFC 3261*. The Internet Society, 2002.

[4] Do Carmo, R.,Masri. (2009). *Código fuente sistema artemisa* [Online]. Available: http://sourceforge.net/ (06.06.2014).

[5] *Código fuente análisis de vulnerabilidades* [Online]. Available: http://www.backtrack-linux.org/wiki/index.php/Pentesting_VOIP (12.11.2014).

[6] *Fortinet* [Online]. Available: http://kb.fortinet.com/kb/microsites/microsite.do (03.04.2015).