HoneyPots Web como Herramientas de Análisis de Ciberataques sobre una Red de Telefonía Móvil

Eduardo Esteban Casanovas [1], Carlos Tapia [2], Santiago Alasia [3], Fabián Polanco [4]
1 Instituto Universitario Aeronáutico,
ecasanovas@iua.edu.ar - 54-351-95-426291
2 Instituto Universitario Aeronáutico,
carlosignaciotapia@gmail.com - 54-351-6874923
3 Instituto Universitario Aeronáutico,
santi.alasia92@gmail.com - 54 9 354 164-2823
3 Instituto Universitario Aeronáutico,
polanco.kick@gmail.com - 54 9 354 164-2823

ABSTRACT

En la actualidad debido al creciente número de ataques informáticos a personas y empresas, constantemente se buscan nuevas maneras de detectar y prevenir ataques o en su defecto mitigarlos, por esta razón surge la necesidad de investigar y aplicar nuevos métodos de defensa para el resguardo de la información; es aquí donde vemos una principal problemática que parte de la sociedad hacia el mundo de la computación.
Por tal motivo, el presente trabajo analiza los conceptos de Infraestructuras Críticas, más específicamente se hace foco en las compañías de telecomunicaciones y en los elementos de red con los que brindan servicios, y se explora la implementación de honeypots y honeynets (hosts y redes señuelo) para prevenir o mitigar ataques informáticos.
La alta dependencia de la sociedad moderna respecto de las telecomunicaciones vuelve a las operadoras en Infraestructuras Críticas para cualquier nación, considerando que son utilizadas masivamente por la población para todas las actividades en cualquier rubro de industria, para las distintas reparticiones y funcionarios de Gobierno, y para los usuarios particulares, volviéndose componentes indispensables para el normal funcionamiento de la sociedad. Puntualmente, se optó por el estudio e investigación de las redes de telefonía móvil como posible blanco de ataques debido a la gran información y datos que se pueden obtener si se llegara a conseguir una puerta de acceso en un punto vulnerable de dicha red; y las redes señuelos como herramienta de defensa, con el fin de analizar y comprender las nuevas tecnologías que utiliza un atacante informático para realizar un ataque y poder determinar el impacto que generaría en el sistema a proteger

Keywords— Honeypots - Ciberataques - Infraestructuras Críticas

1. INTRODUCCION

En el transcurso de la investigación en el campo de las redes señuelo, específicamente de honeypots de servidores web el equipo de trabajo se encontró con la limitación de replicar servidores de aplicaciones web que emulan las tecnologías web existentes, con la consecuencia de que inclusive un atacante novato, fácilmente puede descubrir que estaba atacando a un honeypot y no a un servidor web real. Se destaca que es de gran importancia para un honeypot no ser descubierto como tal.
Particularmente, el objetivo general definido fue conseguir imitar interfaces web de administración de elementos de red de una compañía de telefonía móvil, a los efectos de hacer más atractivo para los atacantes a los objetivos, al mismo tiempo que se logra distraer a los intrusos de los elementos reales y operativos de la red.
A modo de resumen, se listan los objetivos que persiguió el trabajo:
1. Investigar y comprender conceptos de una red de telefonía móvil, seleccionando a la misma como una posible Infraestructura Crítica.
2. Implementar una herramienta capaz de analizar los eventos que ocurren sobre la red.
3. Implementar sensor web sin contexto de infraestructura crítica.
4. Integrar sensor a una herramienta de análisis de datos
5. Evaluar el posible comportamiento de una infraestructura crítica en un ambiente limitado y controlado de pruebas, realizando simulaciones y diferentes casos de uso.
En lo relativo a Infraestructuras Críticas, en la República Argentina el organismo que las regula y atiende es el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), el cual ha definido los siguientes cuatro objetivos principales:
● Servir como repositorio de información relevante relacionada con los incidentes, herramientas y técnicas de Seguridad Informática.

● Promover la coordinación entre los administradores de redes para todas las instituciones públicas a nivel nacional, a fin de prevenir, detectar, gestionar y recuperarse de los incidentes relacionados con la seguridad que afecten sus redes.

● Centralizar la generación de informes respecto a incidentes que afecten las redes gubernamentales y facilitar el intercambio de información a fin de abordarlos de manera más eficaz.

● Interactuar con otros equipos de respuesta ante incidentes en el país y la región.

2. INFRAESTRUCTURA CRÍTICA

La ICIC genera y sigue un plan para el análisis y definición de las Infraestructuras Críticas. Este plan se basa en cuatro pilares: sensibilización, protección de los activos digitales, promoción de la comprensión judicial y académica de la Seguridad de la Información y la Infraestructura de información crítica y fomento de alianzas de seguridad duraderas entre el gobierno, las empresas y las organizaciones de la sociedad civil.
Tomando en consideración que las Infraestructuras Críticas son aquellas de carácter estratégico cuyo funcionamiento es indispensable y no permite soluciones alternativas, implicando su perturbación o destrucción graves impactos sobre los servicios esenciales para la población, los rubros entre los que se reparten estas Infraestructuras son

● Energía
● Industria Nuclear
● Telecomunicaciones y Tecnológicas de la Información
● Transportes
● Suministro de Agua
● Suministro de Alimentos
● Salud
● Sistemas Financiero
● Industria Química
● Espacio
● Recursos
● Administración

Por otra parte, se pasa a describir el concepto de "Operadores Críticos": son las entidades u organismos responsables de las inversiones o del funcionamiento de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como Infraestructura Crítica por proporcionar un servicio indispensable para la sociedad.
Los operadores designados como tales tendrán la responsabilidad de optimizar la protección de las Infraestructuras Críticas por ellos gestionadas. En ese contexto, el equipo de investigación se orienta al análisis de las redes de telefonía móvil.
Adicionalmente, se exploró el concepto de honeypot (equipo señuelo), siendo éste un sistema muy flexible y versátil dentro del abanico de soluciones de Seguridad Informática, que se encarga de atraer y analizar el comportamiento de los atacantes, y que provee al informático forense información extremadamente valiosa para poder llegar a pronosticar cómo serán los ataques futuros y los métodos de protección a desarrollar e implementar.
Luego, la pregunta que puede aparecer es, ¿para qué puede querer una persona atraer atacantes a sus propio sistema?, esto puede resultar muy contradictorio, pero lo que se busca con esta implementación es capturar todo el tráfico de red entrante y conocer todos los detalles acerca de las tendencias y metodologías de ataque de los atacantes así como los fallos de seguridad en nuestra red con el fin de subsanarlos.

3. HONEYPOT

Los honeypots pueden ejecutarse bajo cualquier sistema operativo, generalmente se aplican en sistemas Linux. Los servicios configurados determinan los diferentes vectores de ataque disponibles para que el intruso ponga a prueba y comprometa el sistema.
Estas son algunas de las posibilidades que nos ofrecen los honeypots:

● Desviar y distraer la atención del atacante.
● Detectar y aprender nuevas vulnerabilidades.
● Obtener información sobre el atacante (geolocalización, IP, puertos, etc.).
● Obtener tendencias de ataque y países más atacados.
● Detectar nuevas muestras de malware que aún no se conozcan.
● Recopilar y estudiar tendencias de ataque

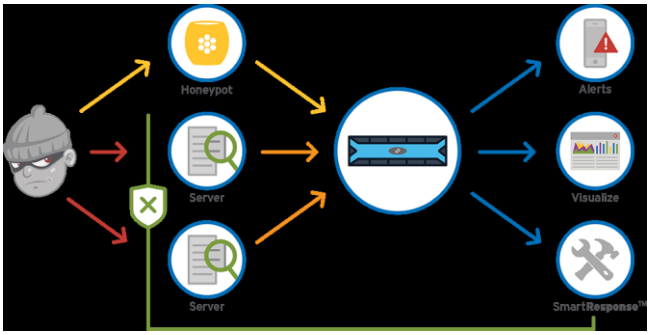

Figura 1: Esquema de un honeypot

Tomando este concepto de honeypot, el equipo comenzó a analizar la infraestructura de las redes de telefonía móvil. Dichas redes, también denominadas redes de celdas o celular son redes formadas principalmente por los siguientes cuatro elementos:
1. Dispositivos móviles: Son los equipos electrónicos que permiten a los abonados realizar llamadas, recibir llamadas, transferir datos y contenidos multimedia con otros dispositivos móviles. Esto es posible a través del envío y recepción de señal de la estación base.
2. Estación base: Es la estación central dentro de una celda, conocida como BTS (Base Transceiver Station), realiza el enlace de radio frecuencia a los terminales celulares, transmite información entre la celda y la estación de

control-conmutación, además monitorea la comunicación de los abonados.

3. Estación de control y conmutación: Conocido comúnmente como MTSO (mobile telephone switching office), cuando aplica tecnología GSM se denomina MSC (mobile switching center), y para redes Wireless Local Loop se denomina XBS. Es el elemento central de la red, sus funciones principales son:

- Coordinar y administrar todas las BTS
- Coordinar las llamadas entre la oficina de telefonía fija y los abonados, así como las llamadas entre los terminales celulares y los abonados, a través de las BTS
- Se encarga de la facturación (billing)
- Dirige el Hand off entre cell site
- Tiene un software de gestión: network management system.

4. Radio canal: Se entiende por Radio Canal al par de frecuencias portadoras más un time slot, que van a servir como canales de tráfico en una comunicación. De estas 2 frecuencias una va a ser la frecuencia de Tx de la estación base y Rx del terminal, la otra frecuencia va a ser la de Rx de la estación base y Tx del terminal. Transportan datos y voz entre el abonado y las estaciones base, cada abonado sólo puede usar un canal a la vez.

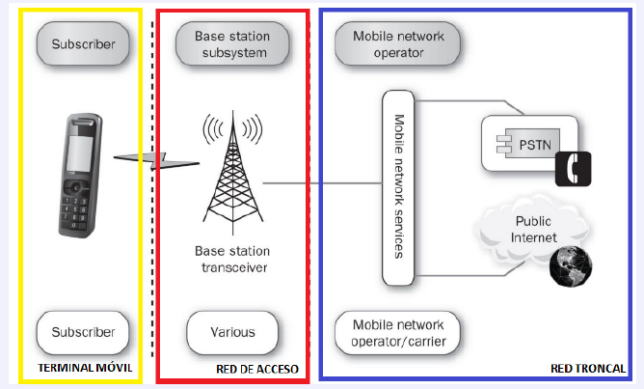

Figura 2: Red de telefonía móvil

4. RED DE TRABAJO

Habiendo sido presentados los conceptos sobre los que se basa el trabajo, el equipo de trabajo pasó a desplegar una implementación de laboratorio para demostrar la utilización de un moderno honeypot de servidor web que emule o imite la interfaz web de administración de una BTS (Base Station Subsystem).

Los elementos utilizados, a los efectos de demostrar la utilidad son:

- Snare: Super Next generation Advanced Reactive honEypot es un proyecto de software el cual se utiliza para clonar sitios web de manera que sirvan como sensores de una honeynet. Este software se integra con Tanner que es otro software encargado gestionar los eventos capturados por Snare. De esta manera se pudo trabajar con la información que obtenida para evaluar ataques y logs de una aplicación web. En esta etapa el objetivo del proyecto fue hacer funcionar Snare para que se pueda obtener un clon de OpenBTS y de esta manera poder establecerlo como honeypot de nuestra red, para que se evalúen posibles ataques.

Figura 3: Prueba de ejecución de Snare

Como se acaba de mencionar SNARE utiliza Tanner para gestionar los eventos capturados para poder trabajar con los datos recopilados y obtener información una vez analizados. Una vez que se concluyó la instalación de SNARE se procederá a la configuración de Tanner, este deberá ser clonado de su repositorio

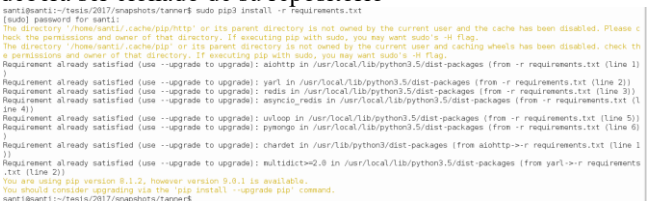

Figura 4: Instalación de requerimientos TARNER

- OpenBTS: Uno de los objetivos principales de este trabajo fue la investigación de posibles ataques a una red de telefonía móvil y poder plantear una posible solución a ello. Luego de una extensa investigación en cuanto la arquitectura de una red móvil se decidió hacer foco en el área de control de radio, es decir, la que se encarga de proporcionar y controlar el acceso de los terminales al espectro disponible, así como también del envío y recepción de los datos. Los sistemas de control utilizados por la mayoría de las empresas de telefonía móvil no se dan a conocer públicamente por lo que el equipo de trabajo se vio en la necesidad de buscar algún sistema de uso libre que cuente con características similares. Por tanto se optó por la utilización de OpenBTS (Open Base Transceiver Station) que es un punto de acceso de GSM basado en software, que permite a los teléfonos móviles compatibles con el estándar GSM hacer llamadas telefónicas sin usar las redes de telecomunicaciones existentes y que, a los fines de este trabajo de investigación, bien puede funcionar como reemplazo de las soluciones de BTS de los grande proveedores comerciales como Nokia, Ericsson o Huawei. OpenBTS es notablemente estable para ser la primera implementación de software libre del protocolo de stack del estándar industrial GSM. Con esto se logró tener una visión más cercana a lo que se refiere un sistema móvil, por lo cual se decidió analizar los diferentes tipos de ataques que

éste puede recibir, para luego plantear mecanismos de defensas a fin de evitar futuros ataques, como se menciona en el planteamiento de los objetivos de trabajo.

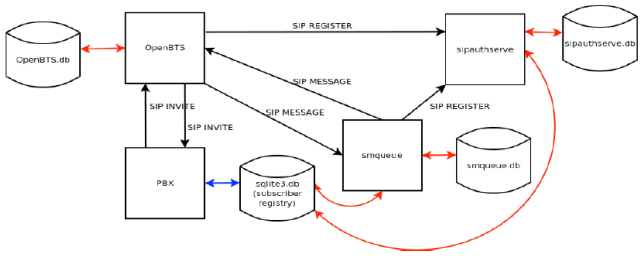

Figura 5: Despliegue de Open BTS

Para instalar la interfaz de usuario que permite gestionar el sistema OpenBTS, primero se deberá clonar el repositorio y luego configurar la base de datos de la siguiente manera

```
DATABASES = {
        'default': {
            'ENGINE': 'django.db.backends.mysql',
            'NAME': 'openbts',
            'USER': 'root',
            'PASSWORD': 'root',
            'HOST': 'localhost',
            'PORT': '3306',
},
'asterisk': {
        'ENGINE': 'django.db.backends.mysql',
        'NAME': 'asterisk',
        'USER': 'root',
        'PASSWORD': 'root',
        'HOST': 'localhost',
        'PORT': '3306',
},
        'smqueue': {
        'ENGINE': 'django.db.backends.mysql',
        'NAME': 'smqueue',
        'USER': 'root',
        'PASSWORD': 'root',
        'HOST': 'localhost',
        'PORT': '3306',
},
        'subscriberregistry': {
        'ENGINE': 'django.db.backends.mysql',
        'NAME': 'subscriberregistry',
        'USER': 'root',
        'PASSWORD': 'root',
        'HOST': 'localhost',
        'PORT': '3306',
}
}
MEDIA_ROOT = '/opt/openbts-webui/webgui/media'
TEMPLATE_DIRS = ("/opt/openbts-webui/webgui/html")
```

- GrayLog: En esencia es un SIEM (Security Information and Event Management). Es posible utilizar esta herramienta para recoger y controlar una gran variedad de registros, pero para este trabajo se limitó el alcance a la recolección de logs enviados desde Snare (específicamente desde su gestor de logs, Tanner).

Componentes Graylog2

- Los nodos de servidor Graylog2: Sirven como procesador que reciben y procesan los mensajes, y se comunican con todos los demás componentes. Su rendimiento es dependiente de la CPU
- Nodos Elasticsearch: almacena todos los logs/mensajes. Su rendimiento es dependiente de la RAM y disco I/O.
- MongoDB: Base de datos no-SQL
- Interfaz Web

Aquí se muestra un diagrama de los componentes Graylog2 (tener en cuenta que los mensajes se envían desde sus otros servidores)

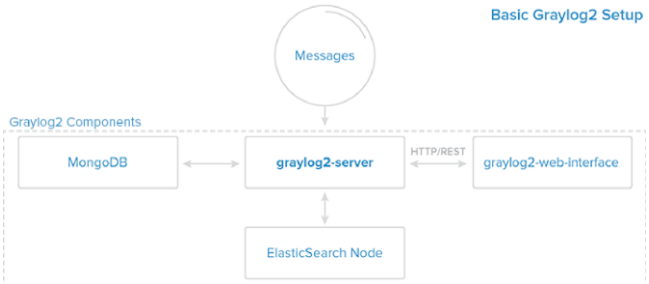

Figura 6: Arquitectura de GrayLog2

Para una configuración muy básica, todos los componentes se pueden instalar en el mismo servidor. Para una configuración más grande, la producción, sería conveniente establecer características de alta disponibilidad ya que si el servidor, componentes Elasticsearch, o MongoDB, experimenta un corte de luz, Graylog2 no reunirá los mensajes generados durante el corte

Figura 7 : Login de GrayLog2

- Servidor NGNIX

Ngnix es uno de los servidores web más populares en el mundo y es responsable de alojar algunos de los sitios más grandes y de mayor tráfico en Internet. Tiene recursos más amigables que Apache en la mayoría de los casos y se puede utilizar como un servidor web o un servidor proxy inverso. En este trabajo NGINX se utilizará para enmascarar el honeypot detrás de un servidor web, es decir SNARE será transparente para el usuario y para los ojos del atacante del sistema.

Esta manera de enmascarar el honeypot evita sospechas del atacante en caso que corrobore el servidor que levanta dicha web clonada, a fin de lograr captar la mayor atención del individuo para que este intente atacarnos.

La infraestructura de laboratorio montada se resume en el siguiente diagrama:

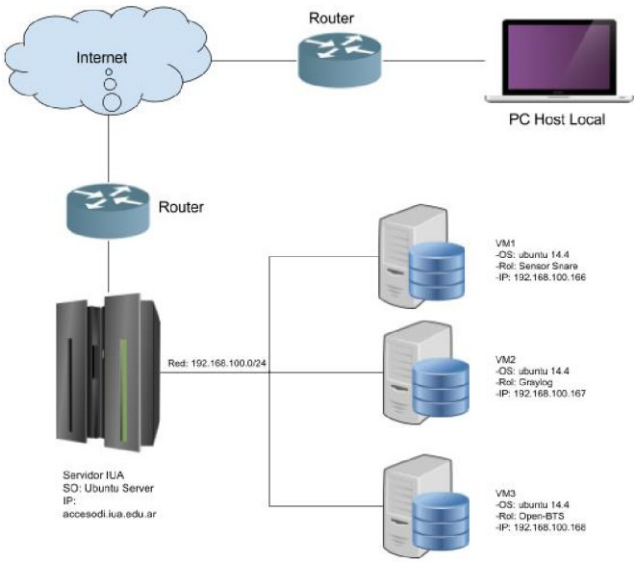

Figura 8: Red montada en el laboratorio

Sobre dicha infraestructura se lanzaron diversos ataques sobre el sensor de Snare, que es el que imita ser la interfaz web de una BTS real, y fue posible registrar los intentos de ataques en el SIEM Graylog. De esta manera, el equipo de investigación pudo monitorear los intrusos y sus intentos de ataques contra una supuesta BTS real, siendo que en definitiva dicho elemento no está brindando servicios de telefonía. Cabe aclarar que las pruebas se condujeron en un ambiente virtualizado que imita ser una implementación básica de una BTS.

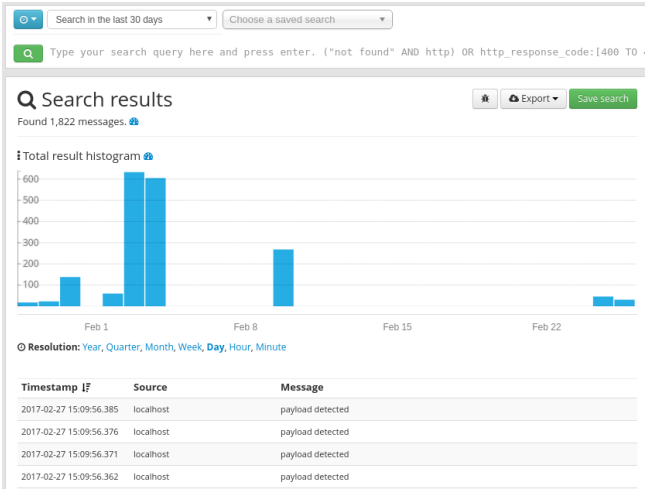

Figura 9: Interfaz de monitoreo y registro de eventos

Se está en condiciones de afirmar que la aplicación clonada y servida por SNARE luce exactamente igual a la interfaz real de administración de Open-BTS y se puede apreciar que el atacante ya ingresa a la aplicación señuelo, por lo tanto, se visualizan los eventos que el intruso realiza sobre la aplicación, dichos logs de eventos se encuentra en el archivo tanner.log y snare.log ubicados en la carpeta /opt/tanner y /opt/snare respectivamente.

Luego de lograr la estabilidad del sensor, a través de los scripts antes mencionados se planteó la integración con MHN (un dashboard que cuenta con varios tipos de sensores como por ejemplo, kippo, glastopf y muchos otros). La funcionalidad de esta herramienta es centralizar logs para visualizar todos los eventos que ocurren sobre de la red en un dashboard para su posterior análisis.

Cuando se inició este trabajo, se creía que iba a resultar una integración sencilla, entre

SNARE, TANNER y MHN, por lo que se comenzó con dicha implementación, luego de varias pruebas se concluyó que dicho proceso era inviable por el tipo de protocolo usado por MHN para la integración de nuevos sensores al dashboard. Hpfeeds es un protocolo liviano, desarrollado en C que se basa en el principio de canales y suscriptores, pero resultó ser un protocolo poco escalable, complejo y demasiado inestable para el sensor SNARE.

De dicho esfuerzo y fruto de investigaciones sobre herramientas que cumplan la misma función que MHN, se decidió implementar Graylog.

Graylog es un sistema de centralización de logs, que brinda la misma funcionalidad que MHN sobre los sensores SNARE y TANNER, con el objetivo de que resulte más escalable para la arquitectura de red planteada en este trabajo.

Una vez inicializado Graylog, se realizó la integración de TANNER. Para integrar el sensor, fue necesario comprender el funcionamiento total, realizando un extenso análisis del código fuente, por lo que se realizó un fork del proyecto original y se introdujeron las siguientes modificaciones. Se agregó una clase que maneje la conexión con el servidor de Graylog

```
import requests
import json
import logging
import http.client as http_client
HOST = "192.168.100.167"
PORT = "12201"
class Graylog():
def __init__(self):
self.endpoint = "http://"+HOST+":"+PORT+"/gelf"
logging.info ('init graylog endpoint
{0}'.format(self.endpoint))
def send_data(self,data):
json_data = json.loads(data.decode('utf-8'))
path =
json_data['response']['message']['detection']['n
ame']
order =
json_data['response']['message']['detection']['o
rder']
requests.post(self.endpoint,
json={'short_message':'payload
detected',"host":"localhost","facility":"test","
_path":path,"_attack_order":
order})
```

Una vez finalizada la sesión de administración en Open-BTS. Se revisaron los registros de eventos en Graylog con fines de analizar al atacante, su perfil y los ataques que éste intentó realizar dentro del sensor web.

5. RESULTADOS OBTENIDOS

Se realizaron diferentes sesiones de análisis y registros de eventos para lograr los resultados que se muestran en la tabla siguiente:

Pruebas realizadas	Resultado
Ataque LFI	Registro de evento y datos del archivo
Ataque SQLi	Respuesta simulada y registro de eventos
Port Scanning	Enmascaramiento del sensor
Ataque XSS	Respuesta Simulada y captura de eventos

Tabla 1: Pruebas realizados sobre la arquitectura

6. CONCLUSION

Como conclusión podemos mencionar que se cumplieron los objetivos propuestos inicialmente, luego de analizar los conceptos de honeypot, Infraestructuras Críticas y de redes de telefonía móvil, logrando una implementación virtualizada y básica de OpenBTS, que si bien no se disponía del hardware necesario para brindar el servicio efectivo de una red de telefonía móvil en un estado operativo y funcional, se hizo foco principalmente, en la seguridad del software de administración y gestión de la red, lo cual permitió demostrar el valor de la inclusión de los honeypots a las Infraestructuras Críticas. Respecto del objetivo número 5, su cumplimiento fue parcial ya que se deberán continuar sumando pruebas, entendiendo que lo probado fue básico. Finalmente, como aspecto positivo adicional se destaca que para todo el trabajo se utilizaron herramientas open-source.

7. TRABAJO A FUTURO

En este proyecto se demostró cómo un sensor web como SNARE y su analizador de eventos TANNER, envían información en tiempo real, hacia un gestor centralizado de logs como Graylog de forma tal que el trabajo a futuro será clasificar esa información en los diferentes tipos de ataques informáticos que existen hoy en día, permitiendo elaborar gráficos y reportes más significativos para la organización que se pretende brindar seguridad.
Además, la Honeynet se puede ampliar a múltiples sensores, no necesariamente webs, ofreciendo mayor cantidad de servicios vulnerables, generando una red más atractiva para un atacante, debido a que esta solución es escalable ya que utiliza un protocolo estandarizado como HTTP a diferencia de otros dashboards como por ejemplo, MHN que utiliza un protocolo que no es estándar.

8. REFERENCIAS

[1] Michael Muter, Felix Freilin, Thorsten Holz, Jeanna Matthews, «A Generic Toolkit for Converting Web Applications Into High-Interaction Honeypots,» 2007.

[2] H. Project, «Know Your Enemy: Honeynets in Universities,» 2004.

[3] «Modern Honey Network,» 2014.

[4] «Super Next generation Advanced Reactive honEypot,» 2015.

[5] «Modern HoneyPot Network: dejando un tarro de miel en internet,» 14 Noviembre 2014. [En línea]. Available: https://www.joanesmarti.com/modern-honeypot-network-dejando-un-tarro-de-miel-en-internet/. [Último acceso: Enero 2016].

[6] h. Project, «Know Your Enemy: Honeynets,» 2006.

[7] M. E. Sánchez, «Implementación de una honeynet para la ciberdefensa de Infraestructuras Críticas,» 2015.

[8] C. Tapia, «HONEYNETS COMO HERRAMIENTA DE PREVENCIÓN,» 2012.

[9] M. Delfino, «Redes anónimas como instrumento para la conformación de un ciber-ataque sobre una infraestructura crítica: Sistema de Radarización de Tráfico Aéreo,» 2015.

[10] H. Project, «hpfeeds,» 2013. [En línea]. Available: https://github.com/rep/hpfeeds .

[11] «Honeynet Project,» [En línea]. Available: https://www.honeynet.org/papers/webapp. [Último acceso: Marzo 2016].

[12] SNARE https://github.com/mushorg/snare

[13] TANNER https://github.com/mushorg/tanner.

[14] Glastopf, ”A dynamic, low-interaction web application honeypot”, Author: Lukas Rist, Co-authors: Sven Vetsch, Marcel Koßin, Michael Mauer, 4 th November 2010.

[15] GSM Network using OpenBTS,Author: Ramón Torres Gomez, Date 5/09/2014

[16] Hacking y Seguridad en Redes de Telefonía Móvil, Author: Mauricio Canseco Torres, Date: 2013.

[17] Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks, Author: Ralf-Philipp Weinmann ,University of Luxembourg. 2015