



# Visualización de incidentes

Modern Honey Network (MHN)

Se atrapan más moscas  
CON UNA GOTTA  
de miel  
que con hiel



# *Honeypot Background*

Utilidad  
Y

Garantía

Patrones  
Y  
Tendencias



*El*  
*problema*  
*Obstáculos*

Ridículamente  
complejas

# Objetivo Proyecto

Implementación de un servidor de intercambio de información a través de la herramienta HPfeed, el cual recolectará la información de los honeypot de red UNAM.

Esta información deberá ser desplegada vía web a través de la herramienta honeymap.



# 5

## *Herramientas Administración*

- **Hpfeeds**
- **Nmemosyne**
- **Honeymap**
- **MongoDB**
- **Dionaea, Kippo y Suricata**

Open source

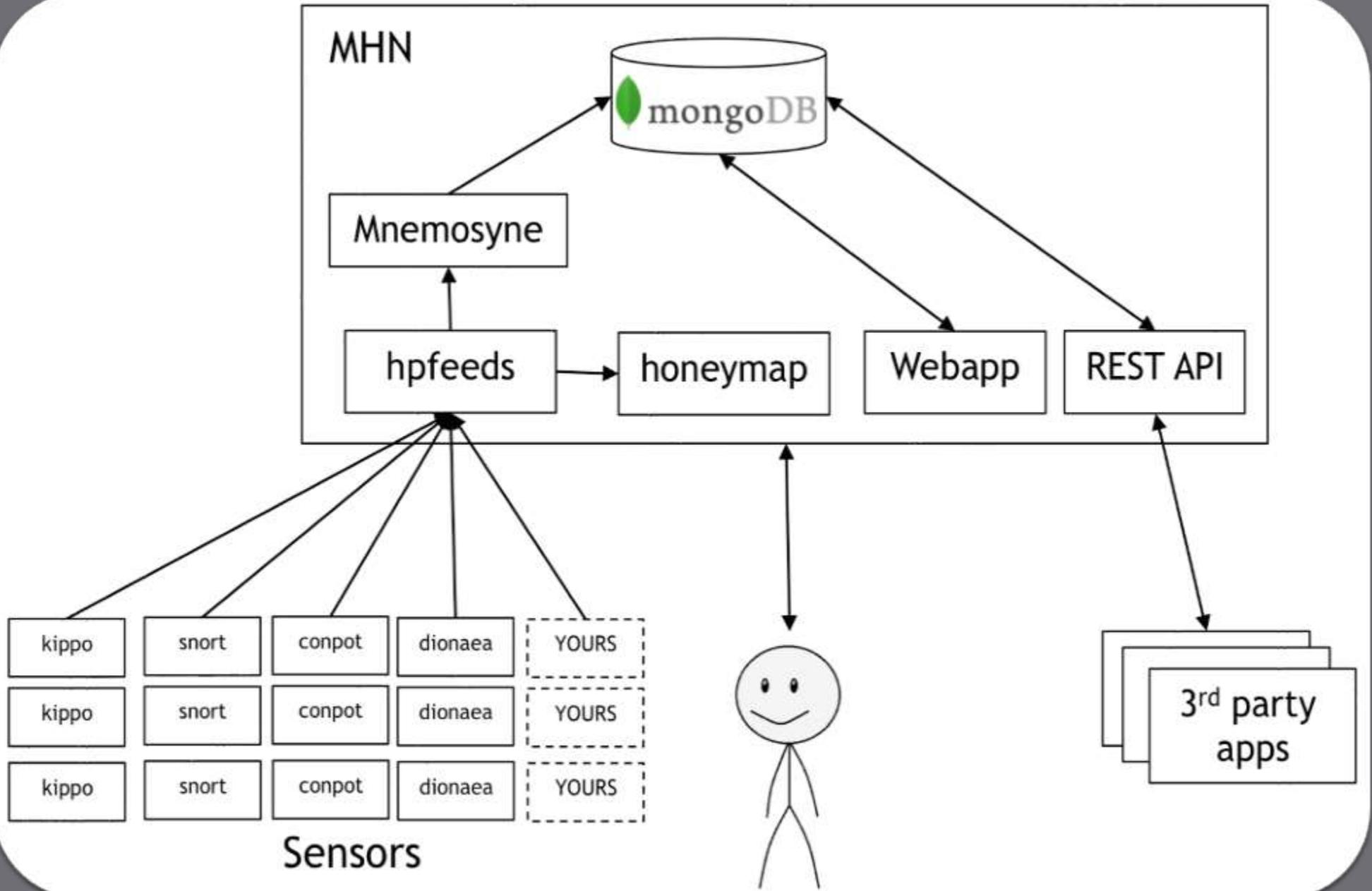


# *Unión*

## *Trabajo en equipo*

1. Despliegue de Honeypots
2. Centralizar el flujo de datos con Hfeeds
3. Organizar y almacenar el resultado con mongoDB.
4. Correlacionar y localizar los eventos con IP Geo Data.
5. Visualización en tiempo real.

*I  
n  
t  
e  
r  
a  
c  
c  
i  
ó  
n*



# Estadísticas de los ataques

Las estadísticas nos permiten conocer:

- Número de ataques en las últimas 24 horas.
- Top 5 IP's
- Top 5 puertos atacados.
- Top 5 honeypots.
- Top 5 sensores.
- Top 5 firmas de ataques

## Attack Stats

Attacks in the last 24 hours: **0**

TOP 5 Attacker IPs:

TOP 5 Attacked ports:

TOP 5 Honey Pots:

TOP 5 Sensors:

TOP 5 Attacks Signatures:

# Mapa de ataques

Mapa que muestra información en vivo de los diversos sensores.

- Ataques en vivo
- Localización geográfica
- Cantidad total de eventos.
- Sensor
- IP
- Hora



# Reporte de ataques

Lista con detalle de todos los ataques registrados:

- ID
- Fecha
- País
- IP origen
- Puerto destino
- Protocolo
- Honeypot

Attacks Report

Search Filters

Sensor: All | Honeypot: All | Date: MM-DD-YYYY

	Date	Country	Src IP	Dst port	Protocol	Honeypot
1	2014-06-17 17:36:57		58.215.43.234	3306	mysql	dionaea
2	2014-06-17 17:36:51		58.215.43.234	3306	mysql	dionaea
3	2014-06-17 17:36:50		125.46.40.21	4188	pcap	dionaea
4	2014-06-17 17:36:44		58.215.43.234	3306	mysql	dionaea
5	2014-06-17 17:36:41		58.215.43.234	3306	mysql	dionaea
6	2014-06-17 17:36:35		58.215.43.234	3306	mysql	dionaea
7	2014-06-17 17:36:32		58.215.43.234	3306	mysql	dionaea
8	2014-06-17 17:36:29		58.215.43.234	3306	mysql	dionaea
9	2014-06-17 17:36:27		198.143.173.183	5060	SipSession	dionaea
10	2014-06-17 17:36:26		58.215.43.234	3306	mysql	dionaea

1 2 3 4 5 ... 37910 37911 »

# Despliegue

Automatización de despliegue:

- Selección honeypot
- Selección de S.O.
- Comando de despliegue
- Script dinámico
- Notas

## Select Script

Ubuntu - Dionaea

## Deploy Command

```
wget "http://192.168.18.248/api/script/?text=true&script_id=7" -O deploy.sh && sudo bash deploy.sh  
http://192.168.18.248 Z5B5c12X
```

## Deploy Script

### Name

Ubuntu - Dionaea

### Script

```
#!/bin/bash  
  
set -a  
set -x  
  
if [ $# -ne 2 ]  
then  
    echo "Wrong number of arguments supplied."  
    echo "Usage: 60 <server_user> <deploy_key>."  
    exit 1  
fi  
  
server_user=61  
deploy_key=62  
  
wget $server_user/static/registration.txt -O registration.sh  
chmod 755 registration.sh  
# Note: this will export the HPF_* variables  
./registration.sh $server_user $deploy_key "dionaea"  
  
# Add ppa to apt sources (Needed for Dionaea).  
apt-get update  
apt-get install -y python-software-properties  
add-apt-repository -y ppa:honeyrat/nightly  
apt-get update
```

### Notes

Initial deploy script for Ubuntu - Dionaea

UPDATE

# Sensores

Lista de sensores registrados:

- Nombre del sensor
- Hostname
- IP
- Honeypot
- UUID
- Número de ataques por sensor

Sensors

	Name	Hostname	IP	Honeypot	UUID	Attacks
1- 	<input type="text" value="ubuntu-kippo-dionaea"/>	ubuntu-kippo	192.168.18.247	dionaea	c8e075bc-7c70-11e5-8066-000c29d31821	1

# Reporte de ataques

Lista de sensores registrados:

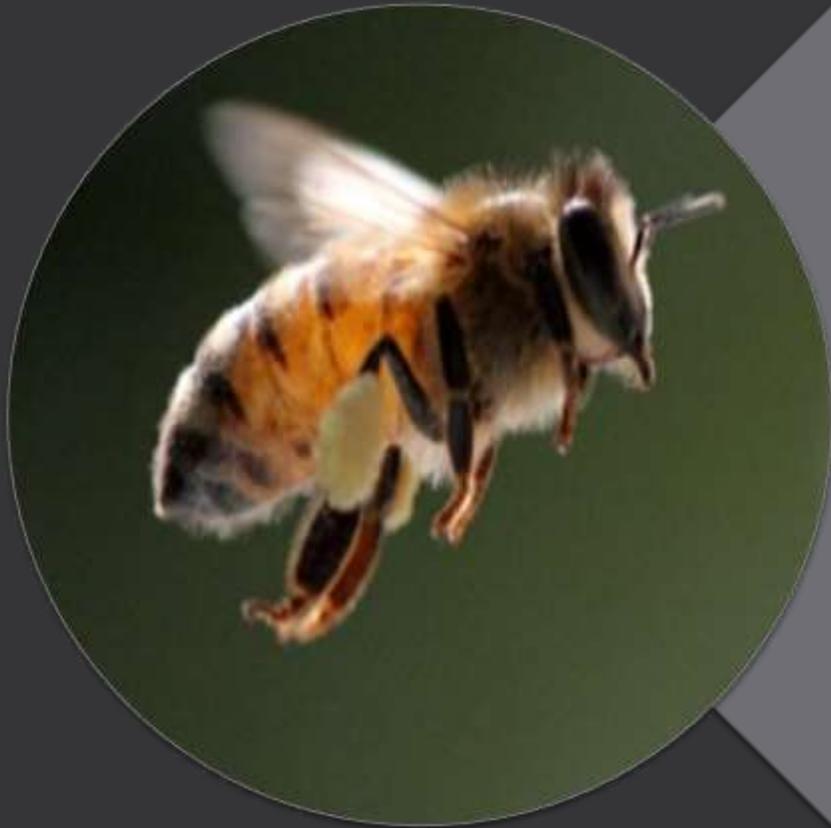
- ID
- Fecha
- Nombre del sensor
- País
- IP fuente
- IP origen
- Puerto origen
- Protocolo
- Honeypot

Attacks Report

Search Filters

Sensor:  Honeypot:  Date:  Port:  IP Address:

	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2015-10-27 06:18:52	ubuntu-Kippo	<input type="text" value=""/>	60.12.1.1	21	ftpd	dionaea



# *Conclusiones*

## *Seguridad rentable*

Monitoreo al alcance de todas  
las organizaciones

# Contacto

Iris González Mortera

Correo: [iris.mortera@sm4rt.com](mailto:iris.mortera@sm4rt.com)

Celular: 55 5189 7504