Visualización de incidentes

Modern Honey Network (MHN)

Se atrapan más moscas
CON UNA GOTA
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**

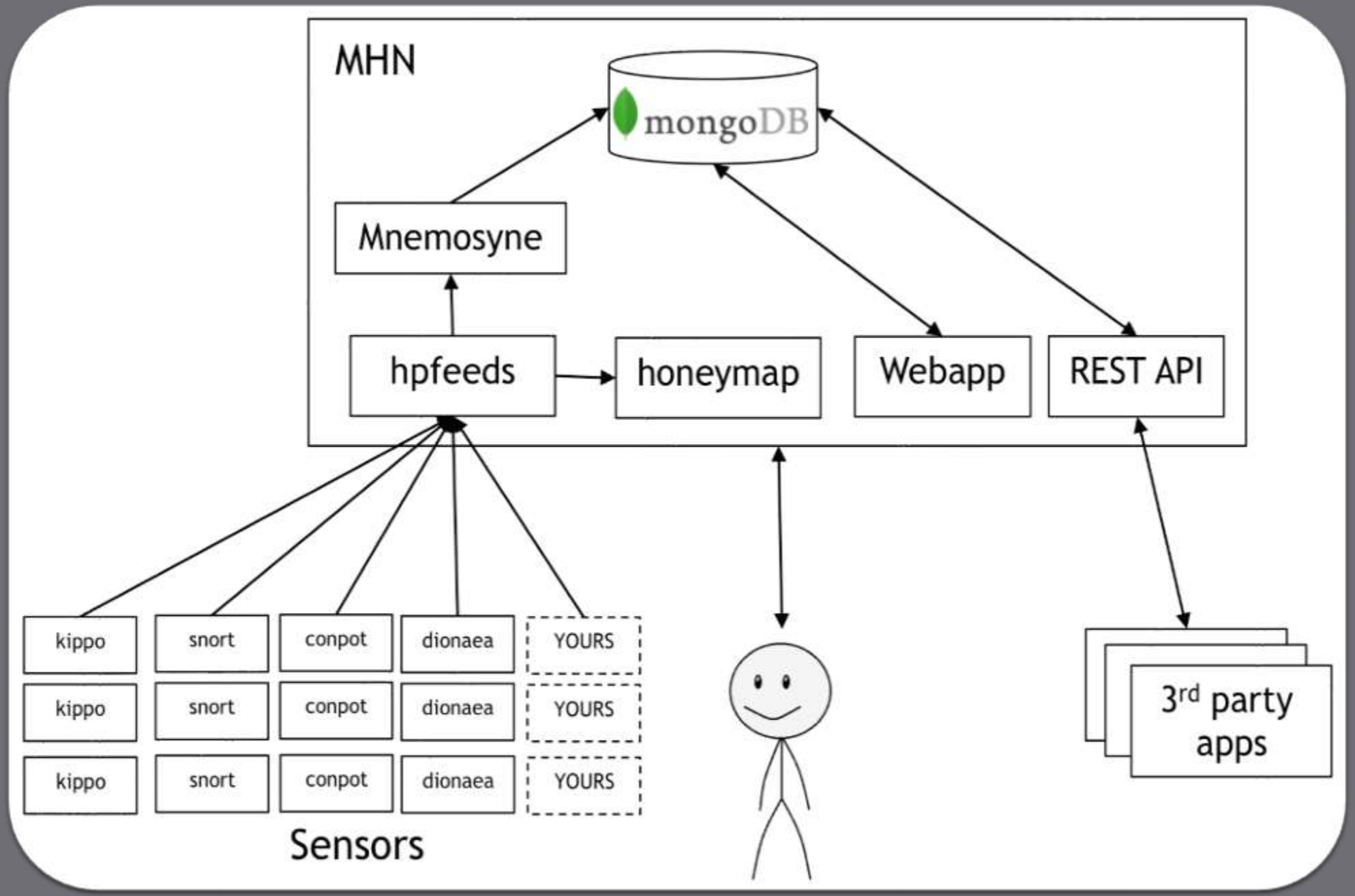
Open source

Unión

Trabajo en equipo

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

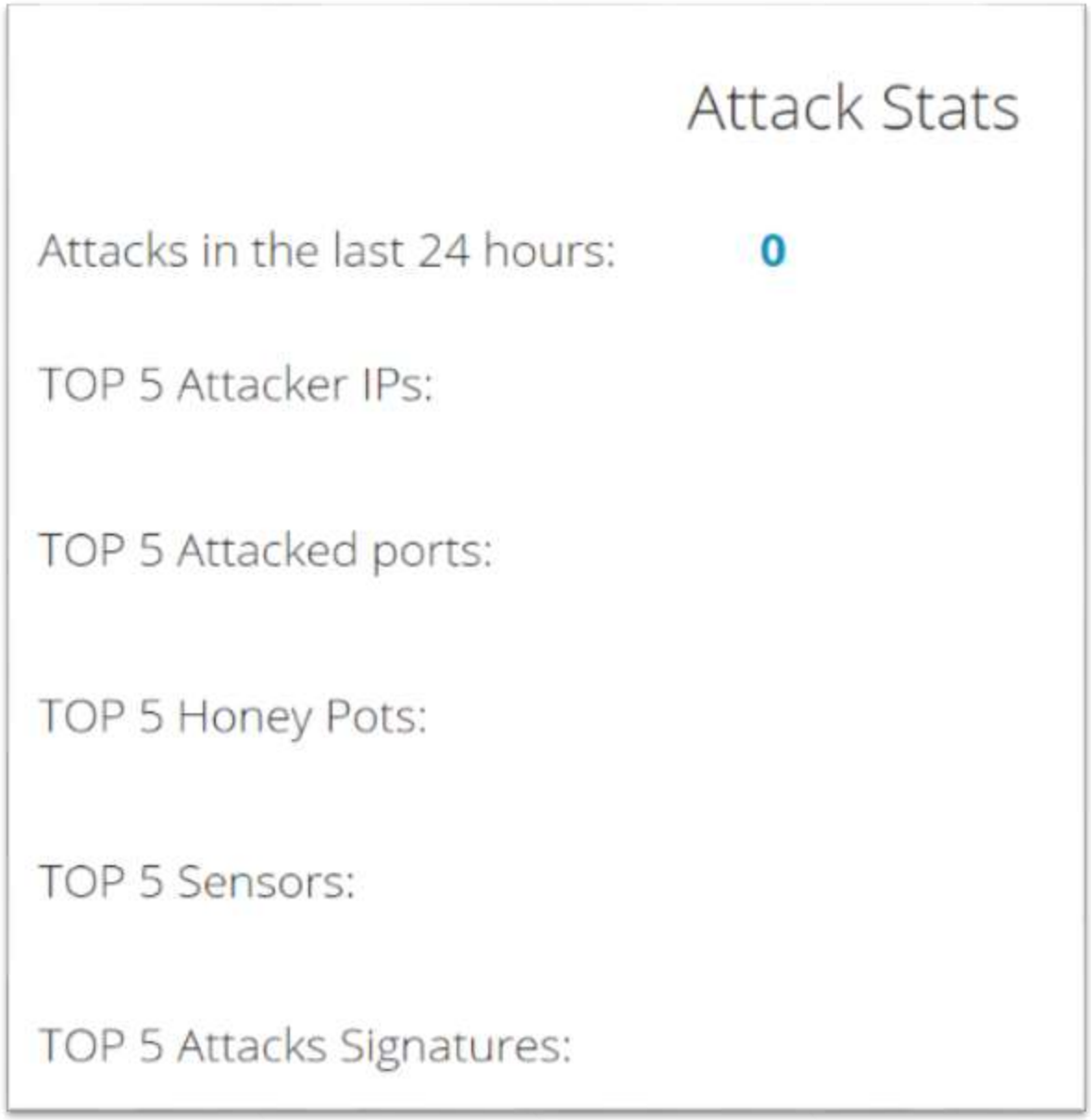
Interacción



Estadísticas de los ataques

Las estadísticas nos permiten conocer:

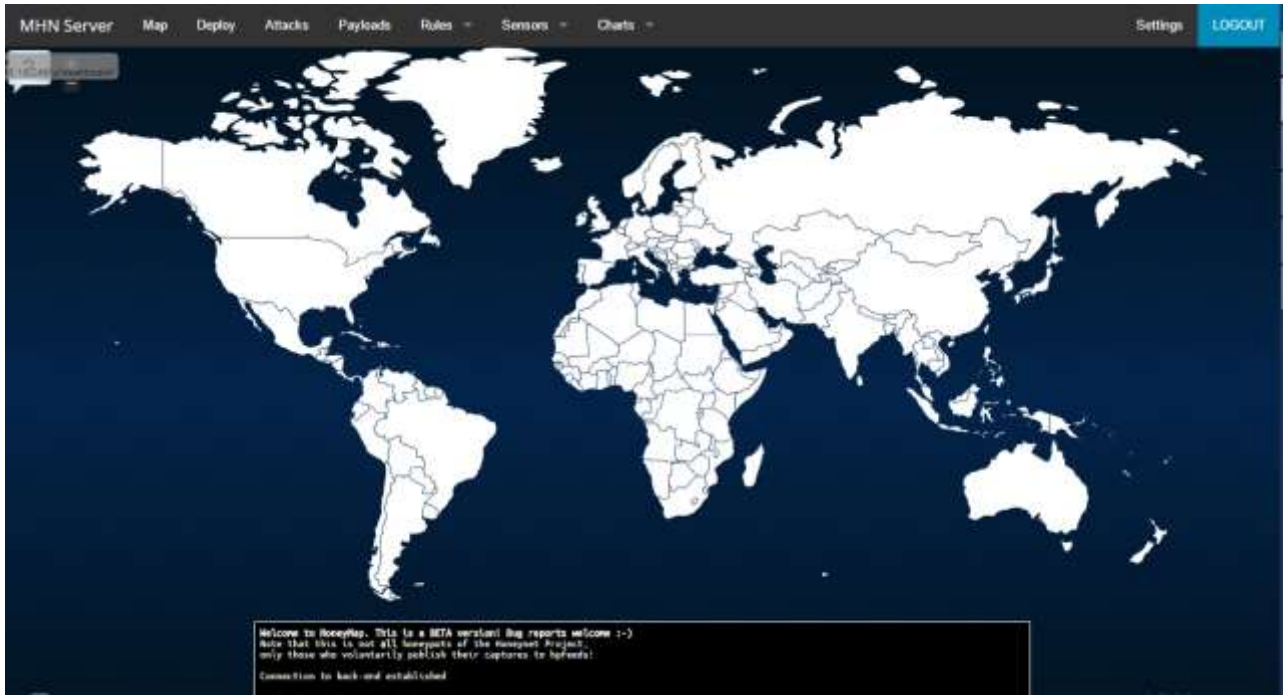
- Número de ataques en las últimas 24 horas.
- Top 5 IP's
- Top 5 puertos atacados.
- Top 5 honeypots.
- Top 5 sensores.
- Top 5 firmas de ataques



Mapa de ataques

Mapa que muestra información en vivo de los diversos sensores.

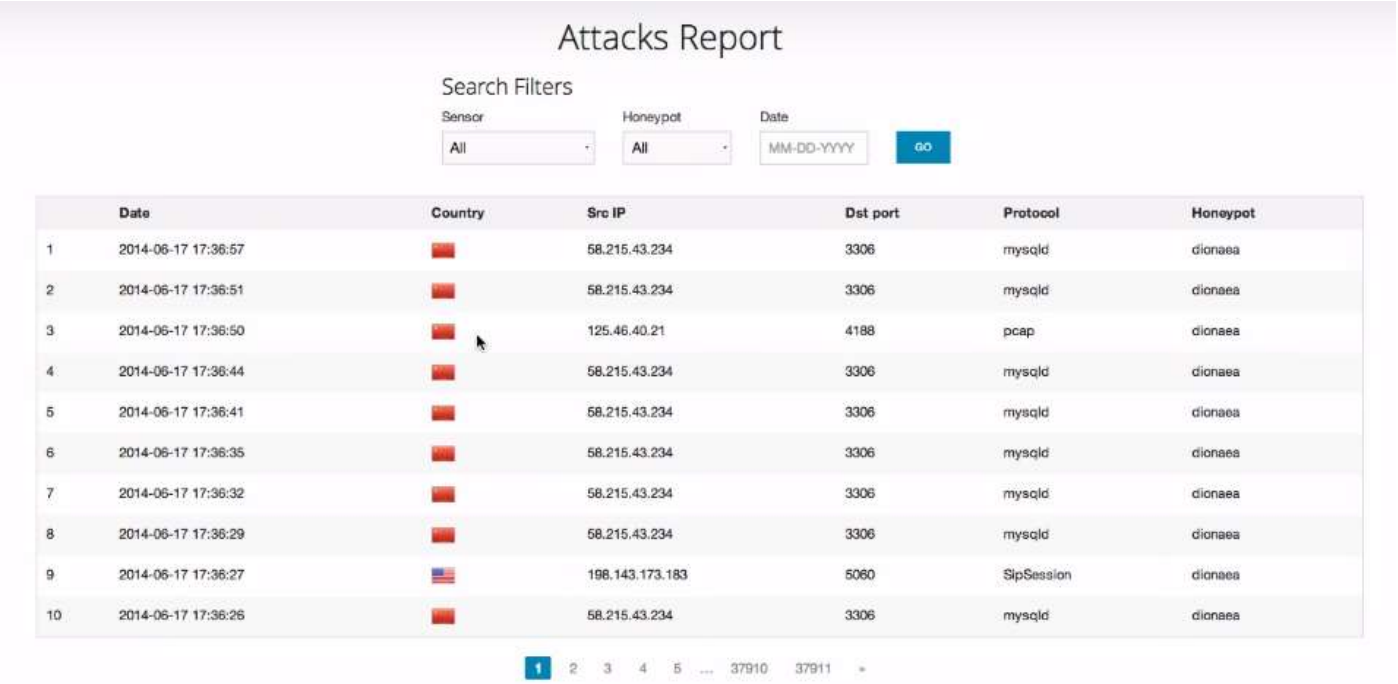
- Ataques en vivo
- Localización geográfica
- Cantidad total de eventos.
- Sensor
- IP
- Hora



Reporte de ataques

Lista con detalle de todos los ataques registrados:

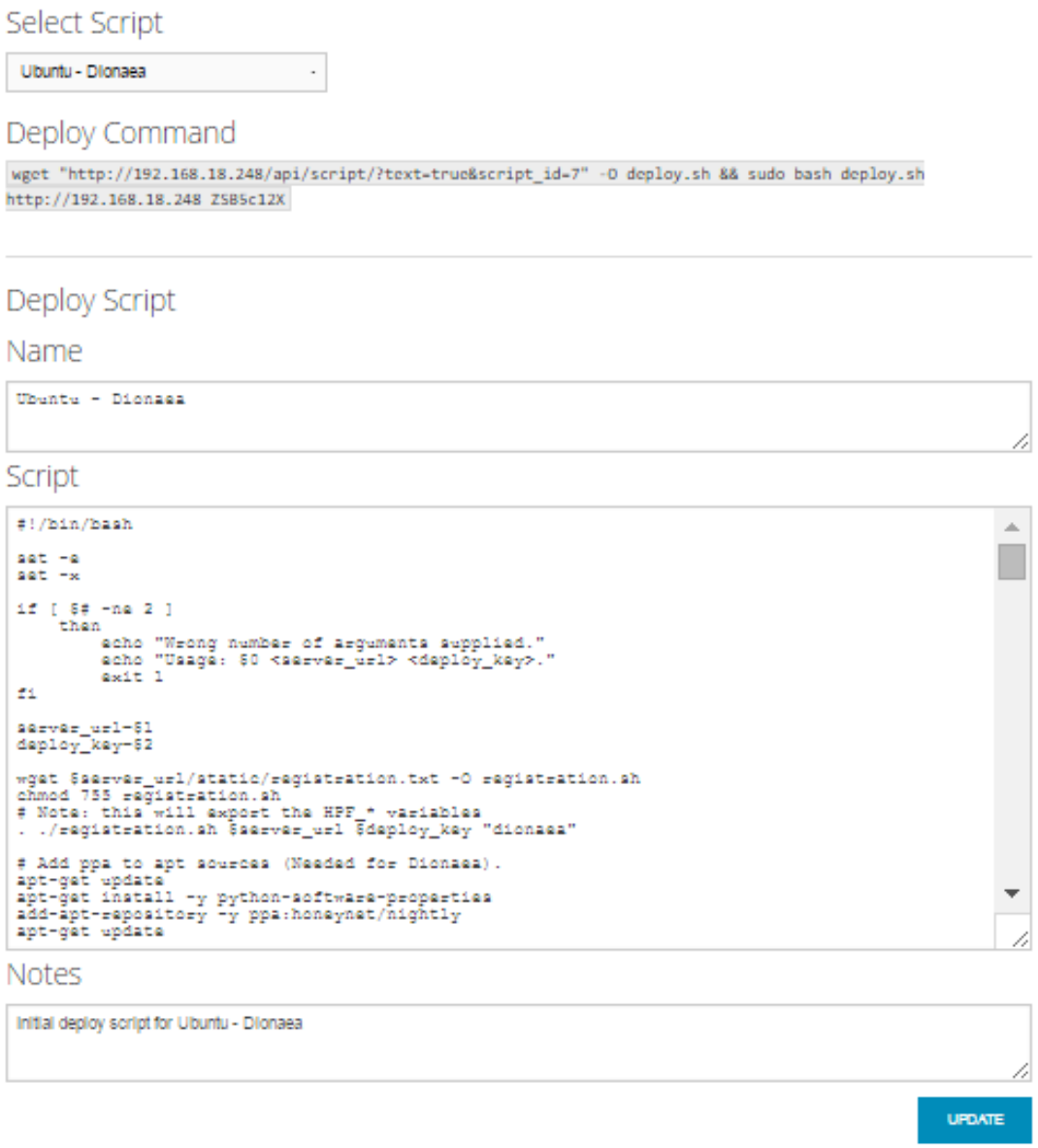
- ID
- Fecha
- País
- IP origen
- Puerto destino
- Protocolo
- Honeypot



Despliegue

Automatización de despliegue:

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



Sensores

Lista de sensores registrados:

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

Reporte de ataques

Lista de sensores registrados:

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

Conclusiones

Seguridad rentable

Monitoreo al alcance de todas las organizaciones

Contacto

Iris González Mortera

Correo: iris.mortera@sm4rt.com

Celular: 55 5189 7504