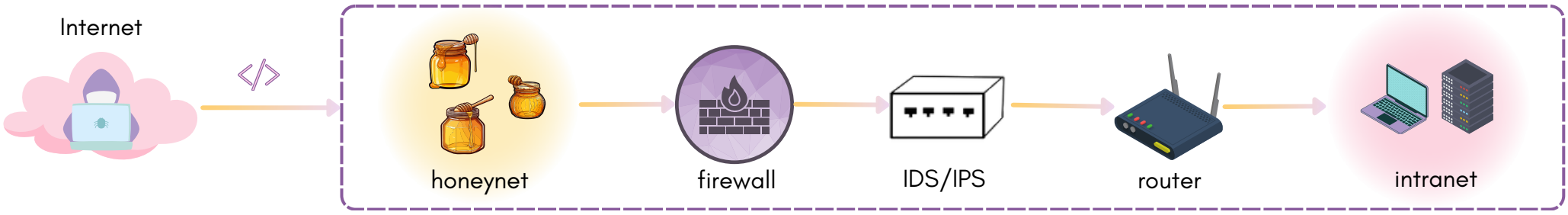
# IMPLEMENTACIÓN DE HONEYPOTS PARA MEJORAR LAS DEFENSAS CIBERNÉTICAS

**Judit López Jiménez**
**Curso 2023 - 2024**

**Trabajo de Fin de Grado de Ingeniería Informática**
**Tecnologías de la Información**

## INTRODUCCIÓN

La implementación de honeypots surge con el objetivo de fortalecer la postura de seguridad de las organizaciones. Estos sistemas tienen la función de atraer a posibles atacantes **simulando vulnerabilidades**. Al registrar la interacción de los atacantes con los honeypots podemos recopilar información sobre **cómo entran a nuestros sistemas y extraen los datos**. Esta información nos permite identificar Indicadores de Compromiso (**IOCs**) que nos ayudan a detectar posibles amenazas.




Infraestructura de red de una organización

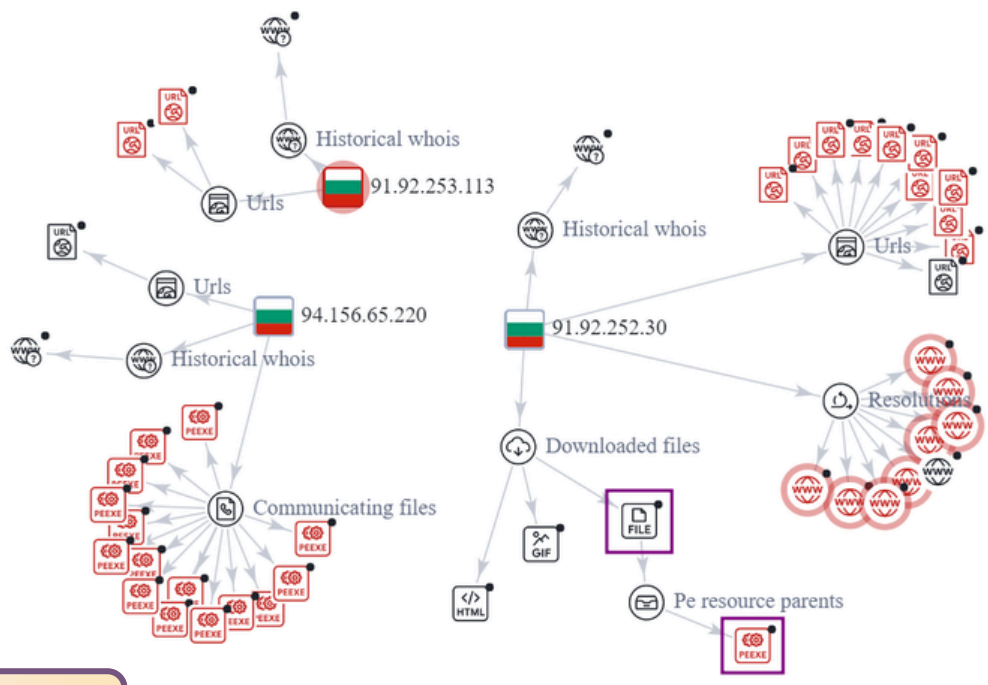
## METODOLOGÍA

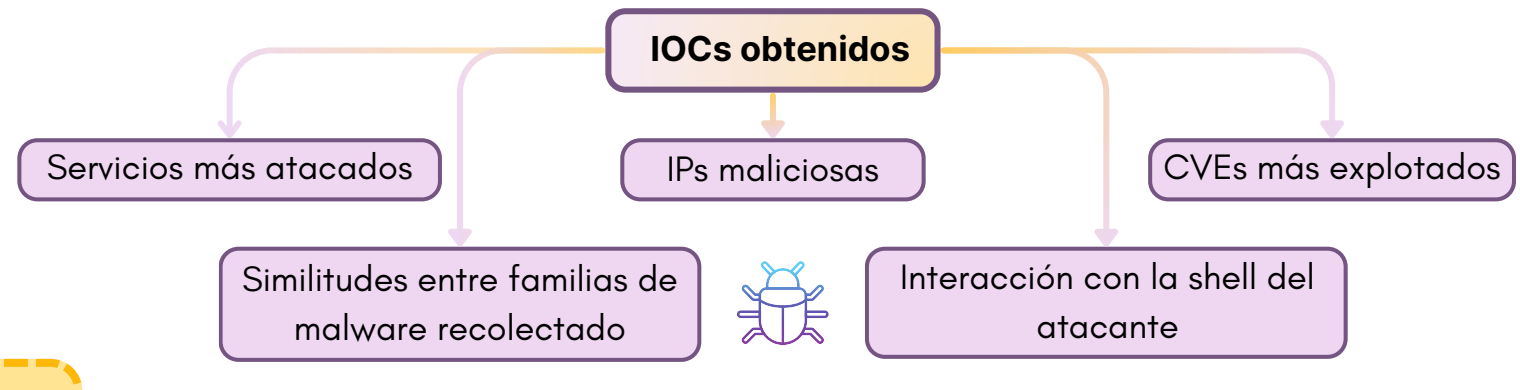
**PLANIFICACIÓN Y PREPARACIÓN** → **DESPLIEGUE DE HONEYPOTS T-POT** → **MONITOREO Y RECOLECCIÓN DE DATOS** → **ANÁLISIS E INTERPRETACIÓN DE DATOS** → **PROPUESTAS DE MEJORA Y CONCLUSIONES**

Metodología waterfall

## RESULTADOS

Entre los IOCs obtenidos se encuentran las direcciones IP que han realizado ataques a los honeypots. Aunque una dirección IP en sí misma no esté catalogada directamente como maliciosa, las redirecciones que realiza hacia otros dominios y archivos pueden ser indicativas de actividad maliciosa. Se ha logrado identificar una dirección IP que estaba atacando los honeypots como parte de una campaña de **fraude bancario en Colombia**. Esta IP está asociada con la web *https:[//]dev-apps-bancolombia.pantheonsite.io*




## CONCLUSIONES

Los honeypots ayudan a **identificar amenazas** existentes. La información obtenida permite **priorizar y enfocar** los esfuerzos de seguridad.

La **adaptación** de los honeypots a los **activos reales** de una organización tiene un gran impacto en la identificación de las amenazas a las que se enfrenta una organización.

**Tutor:** Jordi Pons Aróztegui
Departamento de Ingeniería de la Información y de las Comunicaciones

**Tutor:** Alejandro Sanchez López
SEAT S.A.