JAVIER GARRIDO MONTES

IGNACIO IRURITA CONTRERAS

HONEYPOTS

ÍNDICE

2. ¿QUÉ ES UN HONEYPOT?

- Sistema diseñado para analizar cómo los intrusos emplean sus armas para intentar entrar en un sistema.
- El procedimiento consiste en mantener una debilidad o vulnerabilidad en un programa que motive al atacante a usarlo, de manera que se muestre dispuesto a emplear todas sus habilidades para explotar dicha debilidad y obtener acceso al sistema.

3.CLASIFICACIÓN DE LOS HONEYPOTS

- La mejor manera de diferenciar estos tipos de aplicaciones es por la interactividad. Es decir, hasta qué nivel deja interactuar al atacante con el Honeypot.

Baja Interacción	Alta Interacción
Emulan servicios, vulnerabilidades, etc.	Servicios reales, sistemas operativos o aplicaciones
El riesgo que corren es menor	El riesgo que corren es mayor
Capturan menos información, pero más valiosa	Capturan mucha información. Dependen de su sistema de clasificación y análisis para evaluarlo.

4.DISEÑANDO Y CONSTRUYENDO UN HONEYPOT

- Actualmente existen multitud de herramientas libres que pueden ayudar en el despliegue de honeypots para este tipo de investigaciones o incluso, teniendo los conocimientos necesarios, desarrollar software personalizado.
- Estas herramientas:
  1. Puede ser ejecutadas por línea de comandos,siendo necesario analizar e interpretar los logs que generan para saber que está ocurriendo.
  2. Otras poseen un entorno gráfico desde donde poder visualizar los datos obtenidos.

5.HONEYSTATION

- Origen del ataque
- Nombre del ASN
- Dirección IP del Atacante
- Puerto Atacado
- Número de intentos de ataque
- Tendencias de ataques

5. HONEYSTATION

- Para la visualización de los resultados, la herramienta nos permite 3 tipos de vistas:

    1. **Vista estado del Honeypot:** Muestra una visión del estado actual de la Honey desplegada de forma jerarquizada (Pais - ASN - IP - Puerto - Honey).

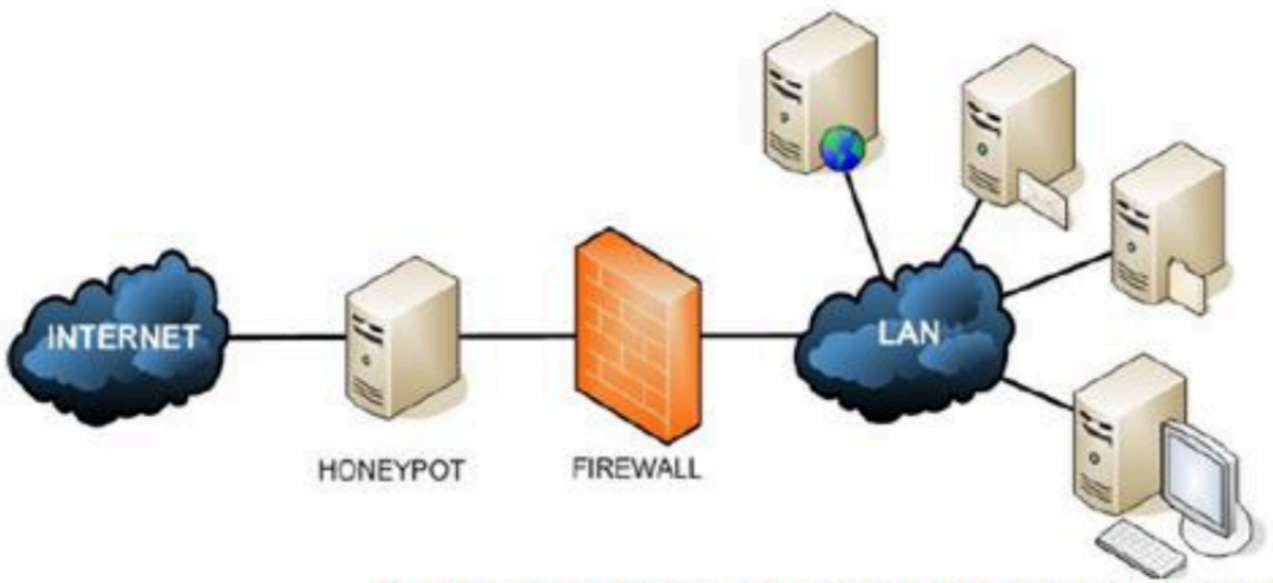
    2. **Vista Geolocalización por país y nivel de ataque:** Muestra el origen de los ataques hacia la Honey, informando del número de ataques registrados y la intensidad del ataque desde un determinado país.

    3. **Vista Geolocalización precisa:** Permite determinar de una forma más precisa la geolocalización del atacante, normalmente a nivel de comunidad, provincia o ciudad.

6.DÓNDE COLOCAR UN HONEYPOT

- Existen 3 zonas referentes:

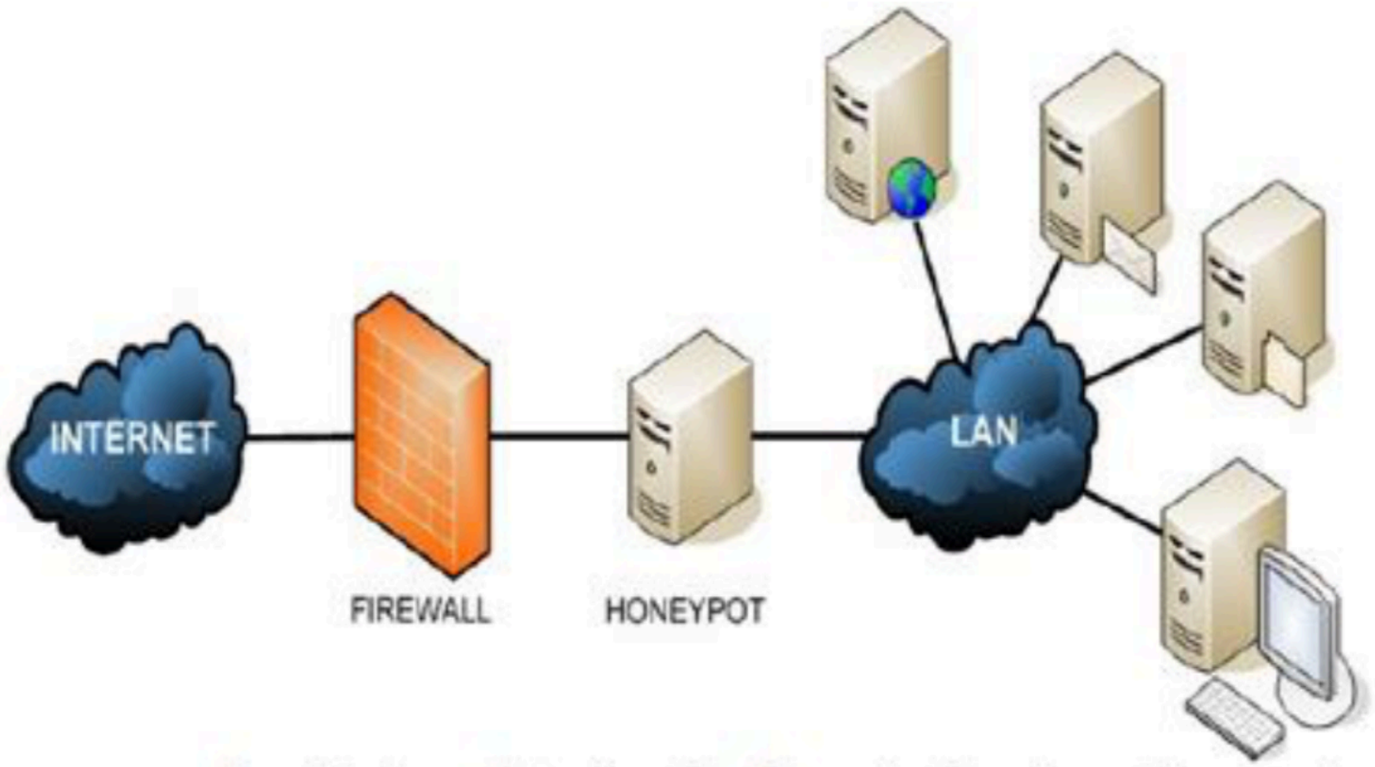
I. Delante del Firewall



Fuente: Inco, diseño e implementacion de un Honeypot

6.DÓNDE COLOCAR UN HONEYPOT

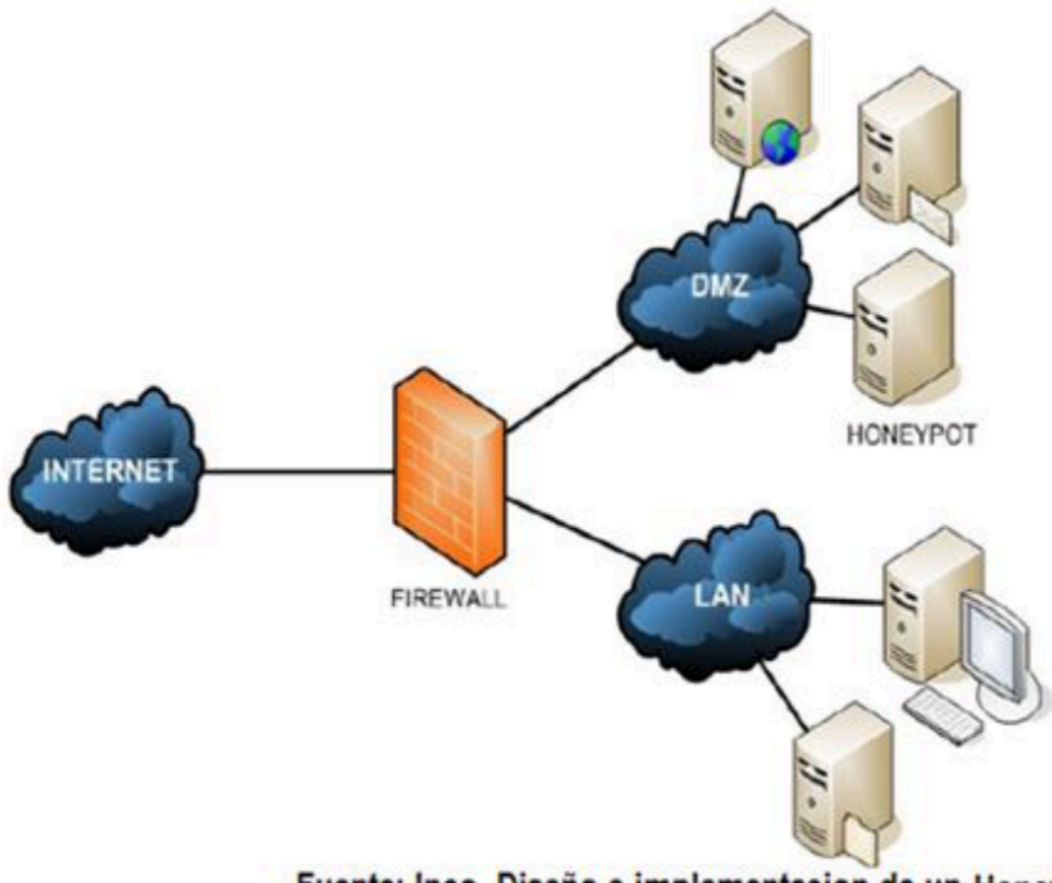
II. Detrás del Firewall



Fuente: Inco, Diseño e implementacion de un Honeypot

6.DÓNDE COLOCAR UN HONEYPOT

III. En una zona desmilitarizada



Fuente: Inco, Diseño e implementacion de un Honeypot

FIN DE LA PRESENTACIÓN