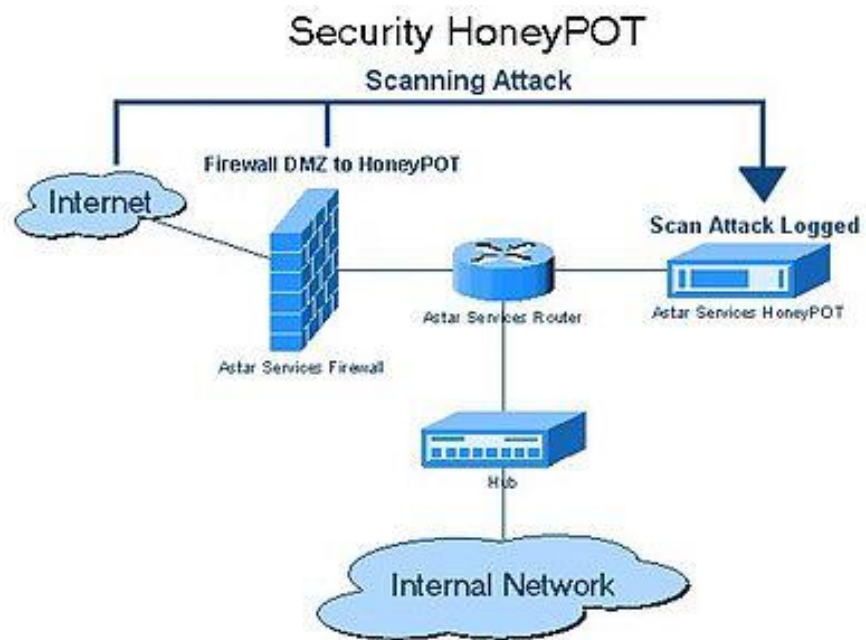


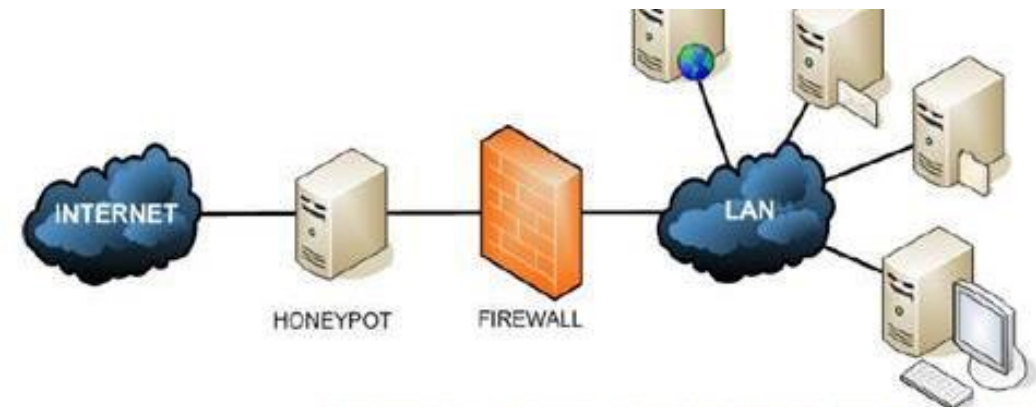
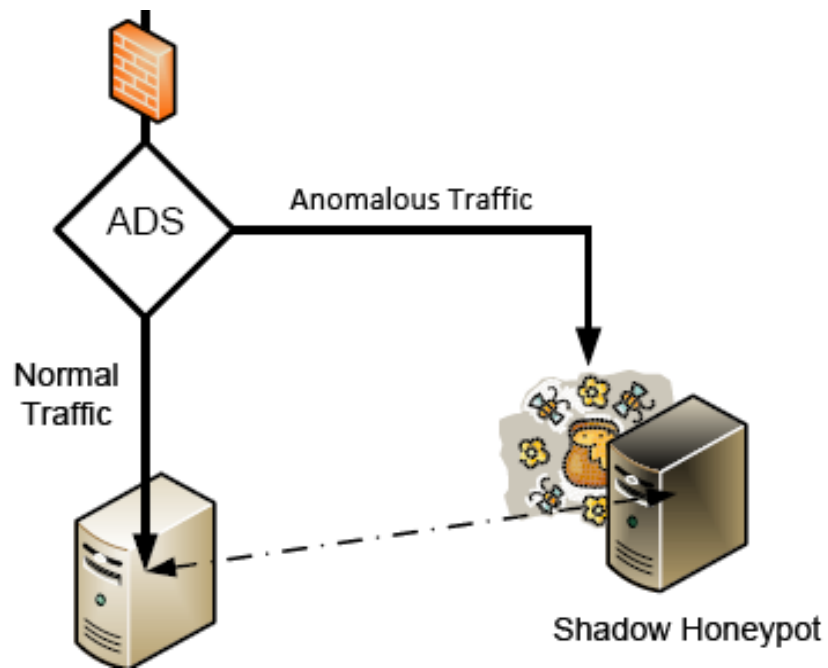
HoneyPot

Presentado por: Miguel González Contreras



¿Qué es un
HoneyPot?

Estructura de HoneyPot



Fuente: Inco, diseño e implementacion de un Honeypot

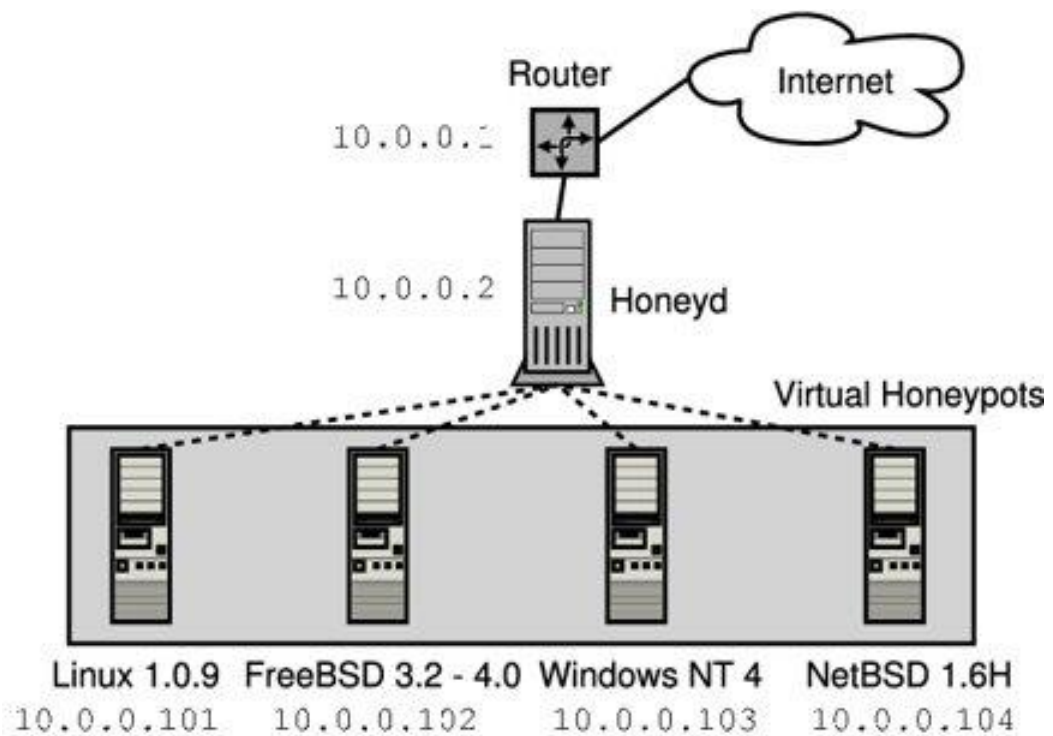
Características

Ejemplos

- Conpot
- Gridpot
- Gaspot
- iHoney

Herramientas

- Honeyd
- HoneyBOT
- Specter
- Kippo



Honeyd

Características

- **Simula miles de hosts virtuales al mismo tiempo.**
- Configuración de servicios arbitrarios vía archivo de configuración simple:
 - Incluye proxy se conecta.
 - Toma de huellas pasivas para identificar hosts remotos.
 - Muestreo aleatorio para escalado de carga.
- Simula sistemas operativos en el nivel de pila TCP / IP:
 - Política de reensamblaje de fragmentos ajustables,
 - Política de escaneo FIN ajustable.
- Simulación de topologías de enrutamiento arbitrario:
 - Latencia configurable y pérdida de paquetes.
 - Enrutamiento asimétrico.
 - Integración de máquinas físicas en la topología.
 - Honeyd distribuido a través de tuning GRE.
- Virtualización de subsistemas:
 - Ejecute aplicaciones UNIX reales bajo direcciones IP virtuales de Honeyd: servidores web, servidores ftp, etc.
 - Enlace dinámico de puertos en el espacio de direcciones virtuales, iniciación en segundo plano de conexiones de red, etc.

Ventajas e Inconvenientes



Ventajas



Trabajan en entornos aislados.



Los datos son concisos y específicos de actividad no legítima.



Producen muy pocos falsos positivos, ya que utilizan servicios no legítimos.



Distracción para los atacantes (creen que están atacando un sistema real).



Obtención de información sobre quién quiere dañar tu sistema de control industrial, su metodología y qué herramientas usa.



Sirve como herramienta para testear la seguridad que posee el sistema.



Puede servir para frustrar a los atacantes y disuadirles de atacar más sistemas.



Inconvenientes



Pueden ser descubiertos por el atacante y ser usados en nuestra contra.



Pueden ser utilizados por el atacante contra otros sistemas distintos al nuestro.



Solo detectan ataques directos al honeyPot (excepto Honeyd).



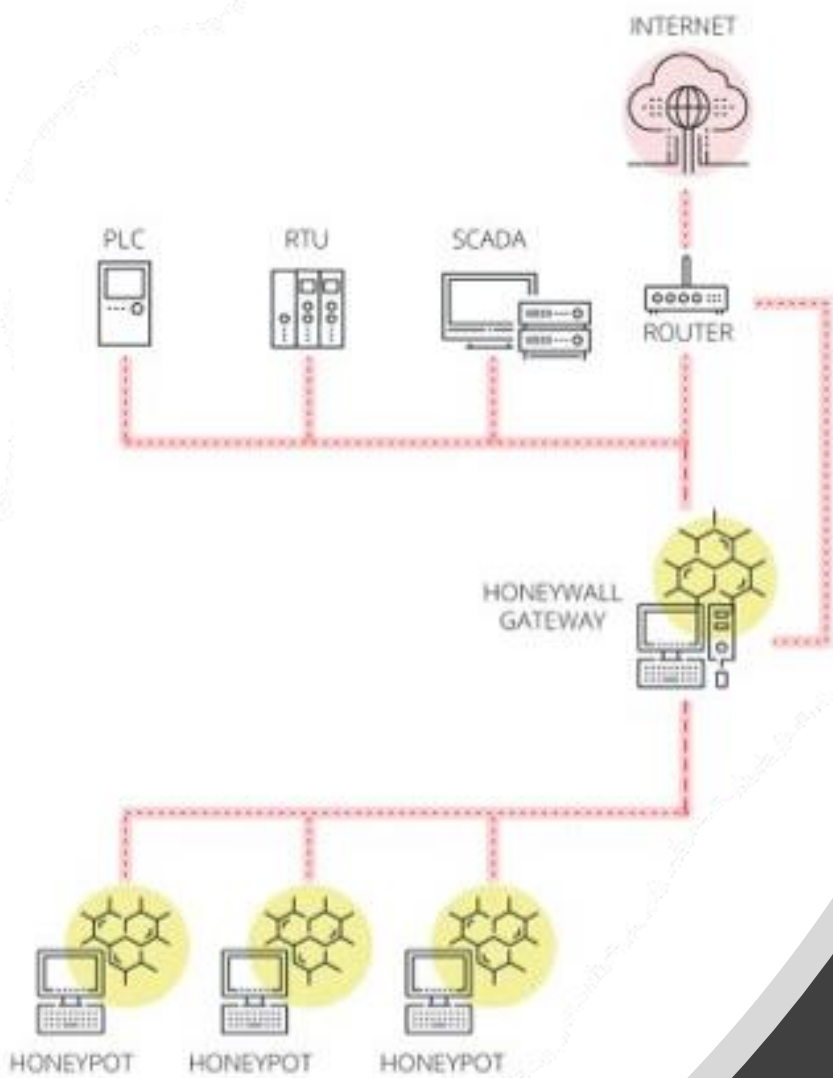
Para implantar un honeyPot se requieren equipos extra (+ coste).



Dificultad de disponer de una simulación realista de dispositivos.



Se necesita del personal necesario (extra) para realizar la monitorización del honeyPot y el análisis de la info obtenida.



HoneyNet

Conclusiones

Fin

<https://github.com/miguegonzalez/SWAP/tree/master/Trabajo%20Final>