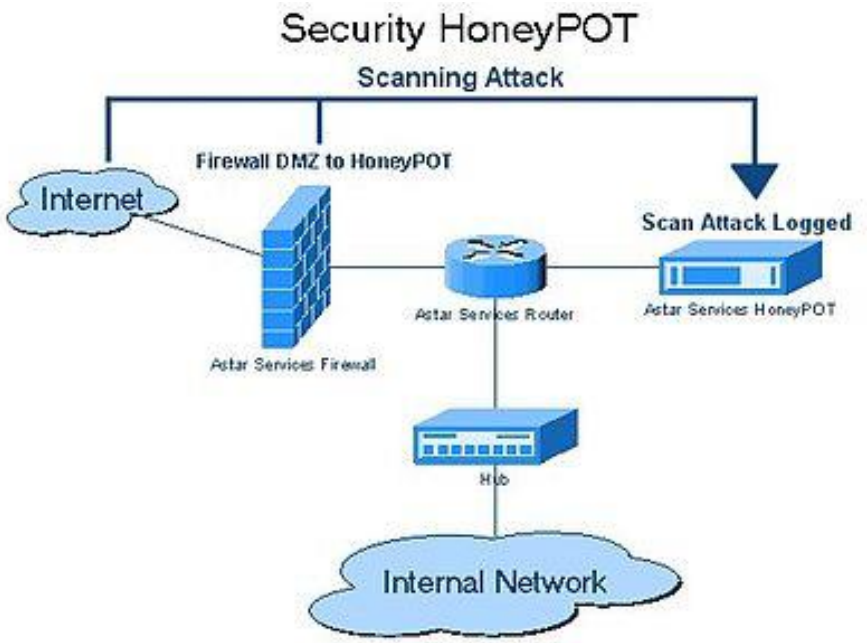
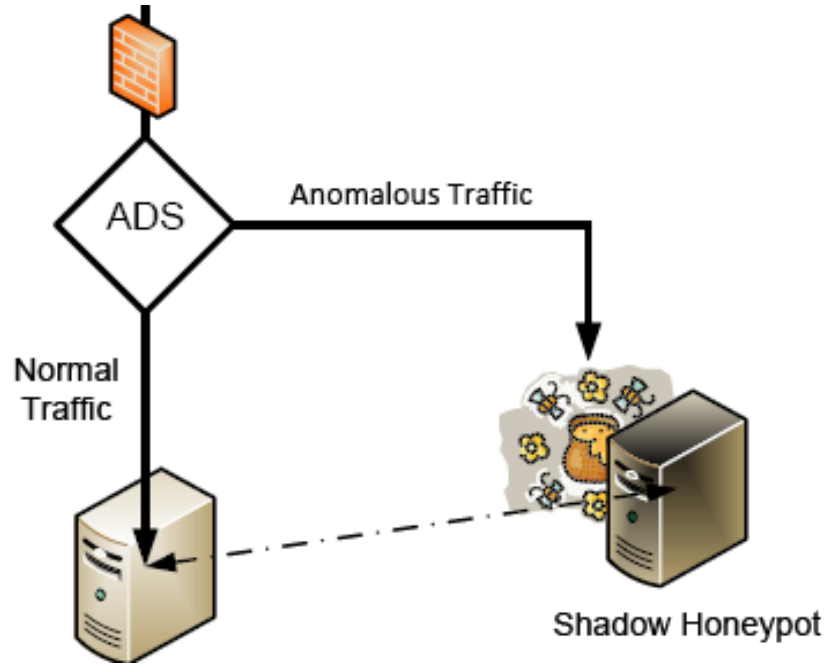
HoneyPot

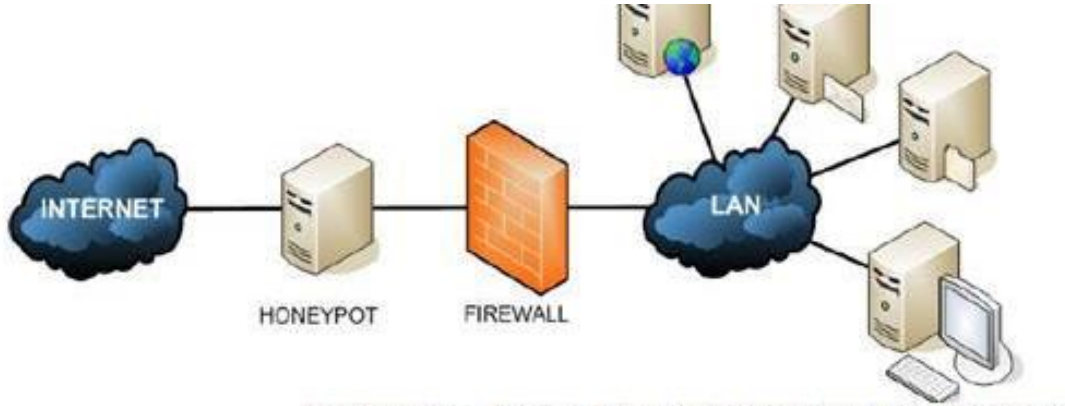
Presentado por: Miguel González Contreras



¿Qué es un HoneyPot?

Características

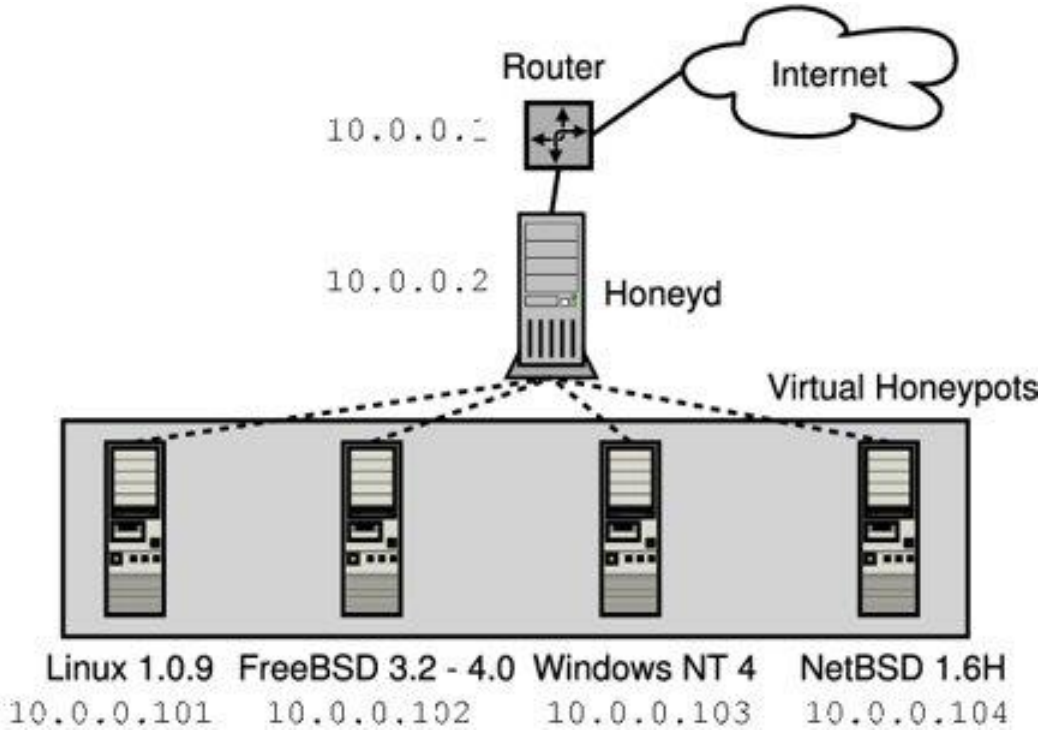




Fuente: Inco, diseño e implementacion de un Honeypot

Ejemplos

- Conpot
- Gaspot
- iHoney


Router
Internet
10.0.0.1
10.0.0.2
Honeyd
Virtual Honeypots
Linux 1.0.9
10.0.0.101
FreeBSD 3.2 - 4.0
10.0.0.102
Windows NT 4
10.0.0.103
NetBSD 1.6H
10.0.0.104

Honeyd

Características

- **Simula miles de hosts virtuales al mismo tiempo.**
- Simula SOs en el nivel de pila TCP / IP: (Política de reensamblaje de fragmentos ajustables y 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:
  - Ejecuta 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.

Conclusiones

Fin

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