Grupo de Seguridad Informática

Honeypots
(parte I)

Honeypots (parte I)

- **Agenda**
  - Definición
  - Ventajas/Desventajas
  - **Motivación**
  - Tipos/clasificación
  - Definición honeynets
  - honeypots vs honeynets (riesgos y cuando usar)

Definición

Un honeypot es un **recurso** que simula ser un objetivo real, el cual se espera que sea atacado o comprometido. Los principales objetivos son el distraer a los atacantes y obtener información sobre el ataque y el atacante
[R. Baumann, C. Plattner]

Un honeypot es un **recurso de seguridad** cuyo valor se basa en ser escaneado, atacado o comprometido.
[L. Spitzner]

Ventajas

- No hay trafico “normal”, toda actividad es sospechosa y potencialmente maliciosa.
  - **no hay falsas alarmas (falsos positivos)**
  - Menos datos a analizar comparado con los IDS
- Puede brindar información valiosa sobre los atacantes.
  - nuevos tipos de malware,
  - herramientas de hacking
  - métodos usados por los atacantes
- Detener, entretener al atacante con sistemas en los que no puede causar daño.

Desventajas

- Hay riesgos potenciales sobre la red de datos y los sistemas de producción de la organización. (dependiendo del tipo de honeypot usado)
- El mantenimiento puede consumir mucho tiempo.
- “narrow view”

¡¡ No es un mecanismo de defensa !!

Motivación

- Tecnología interesante de aplicación en sistemas de producción para mejorar detección
- Es necesario (urgente) comenzar a conocer lo que esta pasando a nivel nacional
- Se esta comenzando a trabajar .... pero falta mucho
- Tecnología que combina distintas disciplinas y áreas de investigación (virtualización, sandbox, análisis forense, etc)

Tipos de honeypots (uso)

- Investigación.
  - Detectar nuevos tipos de ataques y herramientas de hacking.
  - Obtener mayor conocimiento de los atacantes (objetivos, actividades, etc.) y tendencias.
  - Desarrollar nuevas signatures de IDS's
  - Detectar nuevas formas de comunicaciones encubiertas
  - Detectar y analizar nuevas herramientas de DDoS
- Producción
  - Distraer al atacante del objetivo real (ganar tiempo para proteger el ambiente de producción).
  - Recolectar suficiente evidencia contra un atacante (controvertido)

Tipos de honeypots (nivel de interacción)

- **Bajo** nivel de interacción
  - Típicamente soló proveen servicios falsos o emulados
    p.e. listeners, emuladores, **honeyd**, etc.
  - No hay un sistema operativo sobre el cual el atacante pueda interactuar.
  - Fáciles de instalar y mantener.
  - La información obtenida es muy limitada.
  - Minimizan el riesgo considerablemente.

Tipos de honeypots (nivel de interacción)

- Nivel **Medio** de interacción
  - Brinda mayor interacción pero sin llegar a proveer un sistema operativo sobre el cual interactuar.
  - Los demonios que emulan los servicios son mas sofisticados y brindan mayores posibilidades de interacción.
  - El atacante obtiene una mejor ilusión de un sistema operativo real y mayores posibilidades de interactuar y escanear el sistema.
  - El desarrollo/implementación es mas complejo y consume mas tiempo.

Tipos de honeypots (nivel de interacción)

- **Alto** nivel de interacción.
  - Cuentan con un sistema operativo real.
  - Presentan un mayor nivel de riesgo y complejidad.
  - Son objetivos mas “atractivos” a ser atacados.
  - Se obtiene mayor y mejor información de los atacantes.
  - Requiere de mucho tiempo para instalar y mantener.

Tipos de honeypots tabla comparativa

	Low-Involv.	Mid-Involv.	High-Involv.
Degree of involvement	low	mid	high
Real operating system	-	-	√
Risk	low	mid	high
Information gathering	connections	requests	all
Compromise wished	-	-	√
Knowledge to run	low	low	high
Knowledge to develop	low	high	mid-high
Maintenance time	low	low	very high

Baumann – Plattner [Baum02]

Honeynets Definición

- Es una herramienta de investigación consistente en una red diseñada con el propósito de ser comprometida y con mecanismos de control que prevengan el uso de la misma para realizar ataques contra otras redes. [Hoep03]
- Es un honeypot de alto nivel de interacción diseñado principalmente para investigación, con el objetivo de obtener información del enemigo [L. Spitzner]

Riesgos honeypots

- Compromisos de seguridad del Sistema Operativo sobre el cual se ejecuta el honeypot
- Vulnerabilidades del software que implementa el honeypot
- Atrae intrusos/atacantes a la red de servicios o de producción asociada al honeypot.
  (si es detectado)
- A mayor nivel de interacción mayor riesgo.

Riesgos honeynets

- Errores en los mecanismo de contención o en la configuración pueden:
  - La honeynet ser usada para atacar otras redes.
  - Abrir un puerto a la red de la organización
- Un incidente de seguridad asociada a la organización puede afectar la imagen de la misma.
- Que la honeynet sea identificada.

Comparación según nivel de interacción

	Nivel de Interacción	
	Baja	Alta
Instalación	Fácil	Difícil
Mantenimiento	Fácil	Alto consumo de tiempo
Riesgo	Bajo	Alto
Control	No	Si
Datos obtenidos	Limitado	Extensivo

Low x High-Interaction Honeypots [Hoep04]

Posibles usos

- Detectar escaneos y ataques en forma temprana.
- Capturar nuevas herramientas de hacking, gusanos, malware en general, etc.
- Identificar atacantes internos.
- Mejorar el conocimento y tendencias de los ataques/atacantes informáticos (hackers).
- Identificar maquinas infectadas o comprometidas.

Detección, prevención y obtener información

¿ Cuando usar ?

- Honeypot de nivel **bajo de interacción**.
  - Falta de hardware.
  - El riesgo de otro tipo de honeypot es inaceptable.
  - Objetivo:
    - Identificar scaneo y ataques automatizados.
    - Script kiddies con pocos conocimientos.
    - Distraer a los atacantes de los sistemas importantes.
    - Identificar vectores de ataques y tendencias.

¿ Cuando usar ?

- Honeypots de **alto nivel de interacción**
  - El objetivo es observar la actividad y el comportamiento de un intruso:
    - Observar y analizar un sistema “comprometido” real.
    - Conversaciones IRC
  - Se necesita obtener material de investigación o entrenamiento p.e. en:
    - Analisis de “*artifacts*”.
    - Analisis forense.

Grupo de Seguridad Informática

Bibliografía (parte I)

- [Hoep04] C. Hoepers, Honeynets and Honeypots: Companion Technology for Detection and Response, AusCERT2004 Conference, Technical Stream, Mayo 2004.
- [Baum03] R. Baumann, Honeyd – A low involvement Honeypot in Action, Mayo 2003.
- [Baum02] R. Baumann, C. Plattner, Honeypots, Diploma Thesis in Computer Science, Swiss Federal Institute of Technology, February 2002
- [Spit04] Lance Spitzner, Problems and Challenges with Honeypots, Securtyfocus article, Enero 2004.
- [Hoep03] C. Hoepers, K. Steding-Jessen, A. Montes, Honeynets Applied to the CSIRT Scenario, 15th. Anual Computer Security Incident Handling Conference, Otawa, Canada, Junio 2003.