Honeypots

Modelos y procesos de análisis de datos colectados por sensores

Alejandro Blanco

Grupo de Seguridad
Instituto de Computación
Facultad de Ingeniería - UdelaR
http://www.fing.edu.uy/~ablanco

Jueves 24 de Junio, 2010

Plan

Motivación

- No existe la seguridad total en ningún sistema
- Cuanto antes detectemos los incidentes, mejor vamos a poder reaccionar
- Son suficiente los mecanismos tradicionales como IDS o Firewall?
- Que sabemos de los atacantes?

Motivación

- Cuando comenzamos (inicios de 2006), no parecía haber información estadística en UY relativa a incidentes de seguridad. Por ejemplo:
  - Defacement o intrusiones en sitios web en Uruguay
  - Perfil de los atacantes informáticos (origen?)
  - Actividad de Phishing o SPAM
- Los sistemas IDS presentan un alto porcentaje de falsos positivos y dan una visión acotada

Definiciones

Def. Honeypot (R. Baumann, C. Plattner)

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.

Def. Honeypot (L. Spitzner)

Es un **recurso de seguridad** cuyo valor se basa en ser escaneado, atacado o comprometido.

Conceptos a destacar ...

- Se clasifican según:
  - el **recurso** que simulan (Host, Red de Hosts, Tarjeta de Crédito, Servicio)
  - y el **nivel de interacción** que le dan al atacante (Alto, Medio o Bajo)
- Funciona como carnada o sebo para los atacantes
- Existen distintos tipos de servicios que simular: SMTP o Web Server, etc.

Conceptos a destacar ...

- Sirven para:
  - distraer a los atacantes o alertar la presencia temprana (producción)
  - o aprender de ellos (investigación)
- No hay falsos positivos

Trabajos Realizados

- En 2006 comenzamos investigando y experimentando con la tecnología de Honeypot
- Tesis de Grado: "Diseño e Implementación de un Honeypot"(F. Cócaro, M. García, M. J. Roullier - 2007)
- Se realizan las primeras experiencias con la captura y procesamiento de datos estádisticos (2008)

Trabajos Realizados

- Estudio y utilización de Honeypot para la recolección y detección de malware (Honeytrap, Nephentes)
- Utilización de esta tecnología en actividades de enseñanza y capacitación
  - Capacitación sobre Honeypot y *Honeyd* (CSIRTuy 2008)
  - Capacitación Ethical Hacking, laboratorio Herramienta NMap (CSIRTuy 2008)
  - Curso de Capacitación en Ethical Hacking (Ministerio de Defensa Nacional, 2009)

Lineas de Investigación

- Uso de distintas técnicas de virtualizacion para distribución e implantación de Honeypots
- Análisis y Correlación a partír de datos capturados por los Honeypots
- Modelos de datos para uniformizar la gestión y posterior tratamiento de los datos capturados
- Estudio de técnicas y mecanismos de:
  - Correlación
  - Sistemas de Alarmas
  - Sanitización

Conclusiones

- Es una tecnología que demostró poder satisfacer los objetivos iniciales
- Se implementó un primer prototipo de un sistema de captura de datos de **sensores**, con las siguientes características:
  - está basado en Honeypots de bajo nivel de interacción pero escalable,
  - emplea mecanismos que faciliten la reubicación de los sensores,
  - es independiente de la tecnología de Honeypot (sensor) empleada,
  - genera alarmas de la actividad y
  - el monitoreo de los sensores

Conclusiones

- Se trabajó con técnicas de virtualización para la implantación de Honeypots
- Se experimentó con Honeypots para la captura de malware
- Se ha trabajado en la difusión de esta tecnología en el medio local
- Es una tecnología muy útil para la realización de cursos y laboratorios prácticos de seguridad informática

Trabajo futuro

- Estudio de modelos de datos para la representación de los datos recolectados
- Estudio de Algoritmos y técnicas de correlación a partír de datos obtenidos de distintos sensores
  - distintos tipos de Honeypots e implementaciones,
  - Firewall o
  - IDS
- Empleo de técnicas de sanitización de sobre los datos recolectados por estos sensores

Muchas Gracias!
Preguntas?