DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico

Honeytokens

xx-xx

Seguridad de la Información

Integrante	LU	Correo electrónico
Melli, Tomás Felipe	371/22	tomas.melli1@gmail.com
Marco Romano Fina	1712/21	marcoromanofinaa@gmail.com
Milagros Lucía Peris	305/22	miliperis23@gmail.com
Victoria Espil	843/19	victoriaespil99@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

Índice

1 Introducción

Un *honeypot* se define como *un recurso del sistema de información cuyo valor radica en su uso no autorizado o ilícito* [1]. A diferencia de otros mecanismos de defensa cibernética que se centran en **negar el acceso a las amenazas**, el valor de un honeypot reside precisamente en **atraer a los atacantes** para que interactúen con él. Sin la participación activa de atacantes, un honeypot tiene muy poco valor.

1.0.1 Importancia de la decepción

La **decepción** es un concepto fundamental en la implementación de honeypots. Estos sistemas son más eficaces cuando logran **convencer al atacante de que se trata de un sistema real**, logrando así que el atacante interactúe y revele sus tácticas y técnicas. Además de ocultar efectivamente su verdadera naturaleza, un honeypot debe **mantener el interés del atacante** el mayor tiempo posible, de modo que se puedan analizar y descubrir sus métodos de ataque a partir de dichas interacciones.

1.0.2 Limitaciones y evolución

Tradicionalmente, los honeypots son **pasivos** y, por tanto, **poco eficaces para detectar ataques nuevos o complejos**, como los realizados por actores patrocinados por estados. Si no incorporan técnicas de engaño, los atacantes pueden **identificarlos fácilmente** y evitarlos. Para aumentar su efectividad, pueden implementarse **honeypots activos**, que utilizan **respuestas engañosas e inteligentes** para hacer creer al atacante que ha comprometido un sistema real y vulnerable, otorgándole así una falsa sensación de control total.

1.1 Funciones principales

Los honeypots cumplen con tres funciones principales: **detección, prevención e investigación** [2].

1.1.1 Detección

Una de las mayores ventajas de los honeypots frente a otras herramientas de seguridad es su **baja tasa de falsos positivos**. Como los usuarios legítimos no interactúan con ellos, la posibilidad de detección falsa es prácticamente nula. Esta característica les permite **detectar ataques de tipo "zero-day"** con mayor precisión que otras soluciones tradicionales.

1.1.2 Prevención

La función de **prevención** se basa en la capacidad de los honeypots de **desviar y contener a los atacantes** lejos de los sistemas reales. Al actuar como **señuelos**, los honeypots engañan al adversario haciéndole creer que ha encontrado un objetivo legítimo, mientras que en realidad está interactuando con un entorno controlado. De esta forma, los honeypots contribuyen a **reducir el impacto y el alcance de los ataques**, al mismo tiempo que permiten reforzar la seguridad del sistema principal mediante la observación de las tácticas empleadas.

1.1.3 Investigación

Finalmente, la función de **investigación** está orientada a la **recopilación y análisis de información** sobre los atacantes. Los honeypots permiten estudiar en detalle las **técnicas, tácticas y procedimientos (TTPs)** utilizados, así como identificar nuevas vulnerabilidades o comportamientos emergentes. La información obtenida se utiliza para **mejorar las estrategias de defensa, ajustar políticas de seguridad y desarrollar contramedidas más eficaces**. En el ámbito académico y de ciberinteligencia, esta función es fundamental para comprender la evolución del panorama de amenazas y fortalecer la postura defensiva de las organizaciones.

1.2 Selección del tipo de honeypot

Elegir el tipo adecuado de honeypot es una decisión clave que debe tomarse tras evaluar diversos factores críticos:

1. **Estado de la red:** Es esencial analizar la topología, el tamaño y los activos críticos de la red. Un *honeypot de baja interacción* puede ser ideal para redes pequeñas o con recursos limitados, mientras que un *honeypot de alta interacción* es más apropiado en entornos complejos y con mayores recursos.

2. **Disponibilidad de recursos:** Los honeypots de alta interacción, al emular completamente sistemas reales, **requieren más hardware y personal** para su administración, a diferencia de los de baja interacción.

3. **Panorama de amenazas:** La elección del honeypot debe alinearse con los **vectores y tácticas de ataque predominantes** en la red. Diseñar honeypots que simulen las estrategias de los adversarios potenciales puede ofrecer **información valiosa** y mejorar significativamente la seguridad general del entorno.

1.3 Clasificación según el propósito

Los honeypots pueden clasificarse de acuerdo con su objetivo principal:

1. **Honeypots de Investigación:** Diseñados para **recopilar y analizar datos** sobre las técnicas, tácticas y motivaciones de los atacantes. Se utilizan principalmente por investigadores y analistas de amenazas para estudiar **nuevas vulnerabilidades y tendencias emergentes**.

2. **Honeypots de Producción:** Se integran en redes operativas reales con el propósito de **distraer y desviar a los atacantes** lejos de los sistemas críticos. Funcionan como **señuelos** que protegen los activos legítimos y mejoran la seguridad operativa general.

3. **Honeypots de Alta Interacción:** Emulan de forma realista sistemas y servicios completos, permitiendo **interacciones extensas** con los atacantes. Proporcionan información detallada sobre las técnicas y estrategias de ataque, aunque su **gestión es más compleja** y requiere mayores recursos.

4. **Honeypots de Baja Interacción:** Simulan servicios con **funcionalidad limitada**, lo que reduce el riesgo de exposición a vulnerabilidades. Aunque brindan menos datos que los de alta interacción, son **más fáciles de implementar y mantener**, siendo útiles en diversos escenarios.

References

[1] Consultado en: LEARNING CYBERATTACK PATTERNS WITH ACTIVE HONEYPOTS

[2] Consultado en: *Deception in Cybersecurity* A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance