A continuación se muestra una tabla comparativa entre 17 diferentes honeypots, los criterios de evaluación se definieron en: Última fecha de actualización, vulnerabilidades, tipo de interacción y soporte académico. Adicionalmente existe un campo de comentarios donde se destacan rasgos relevantes de cada honeypot.

Las características deseables en los honeypots son: emulación de servicios, captura de tráfico web, exposición de vulnerabilidades.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre** | **Última actualización** | **Vulnerabilidades** | **Tipo interacción** | **Soporte académico** | **Comentarios** |
| LaBrea | 2003-10-30 | Gusanos informaticos. | No especificado | * Citado en: Virtual honeypots: from botnet tracking to intrusion detection.  The honeynet project: Trapping the hackers.**LaBrea**:“Sticky” **Honeypot** and IDS | Su última actualización se realizó hace 15 años.  Su diseño está enfocado en obtener información acerca de gusanos informáticos lo cual no es el objeto de estudio del proyecto. |
| HoneySink | 2011-08-31 | Sink | No especificado | No encontré | Es un honeypot tipo sink Los honeypot tipo sink sirven para detener el flujo de tráfico que se dirige a páginas maliciosas.  No representa mayor utilidad para la captura de información.  No tiene características relevantes para nuestro proyecto. |
| KFSensor | Soporte actual | Emulación de servicios | Alta | **KFSensor** overview 3 citas. Diferentes artículos pero con pocas citaciones. | Capacidad de emular servicios, Capturar trafico, Enviar alertas y genera reportes.  Es un honeypot bastante completo tiene todas las características necesarias para el desarrollo del proyecto |
| Honeyd | 2008-12-4 | Kuang2  mydoom  telnet emul  pop3  iis  ftp  smpt | No especificado | Developments of the **honeyd** virtual honeypot**citado 39 veces** | Está diseñado para vulnerabilidades importantes en años pasados.  No tienes soporte y no está actualizado.  No tiene los requerimientos necesarios para nuestro proyecto. |
| UDPot | 2014-3-18 | Sinkhole  DSN emulator | Configurable | No se encontraron citaciones | Honeypot simple. Funciona como sinkhole y emulador de DNS |
| Conpot | 2018-1-11 | HTTP  SMPT  MODBUS | Baja | **Conpot** ics/scada honeypot8 citaciones | Desarrollado bajo HoneyProject por lo tanto tiene un soporte de investigación. Aún se encuentra en desarrollo y tiene módulos para emular diferentes servicios. Permite captura del tráfico. Falta algunas características para el desarrollo del proyecto |
| Bifrozt | 2016-3-17 | No especificado | No especificado | No se encontraron citaciones | No existe documentación acerca de este honeypot. |
| Beeswarm | 2017-1-17 | Observa la diferencia entre tráfico esperado y tráfico actual | No especificado | No se encontraron citaciones | El proyecto fue descontinuado y su página se encuentra caída por lo cual no se pudo obtener más información. |
| Bait and Switch | 2003-09-28 | Redirecciona el tráfico malicioso hacia el honeypot. | No especificado | No se encontraron citaciones | Enfocado a un ámbito empresarial que busque generar información para I&D. |
| Artillery | 2017-12-19 | Combinación entre honeypot y sistema de detección.  Monitorea más que generar información | No especificado | No se encontraron citaciones | Sistema de monitoreo.  Linux |
| Slimp-Honeypot | 2013-5-27 | Captura información de puertos y trafico en general. | Baja | No se encontraron citaciones | Se basa en un sistema simple de escucha. |
| HoneyWRT | 2015-4-14 | Remote Desktop Protocol (RDP) (TCP/3389) Virtual Network Computer (VNC) (TCP/5900) Fake Shoutcast Server (TCP/8000) Tomcat Admin Page /manage/html (TCP/8080) Microsoft SQL Server (MSSQL) (TCP/1433) Fake Telnet Server (TELNET) (TCP/23) | Baja | No se encontraron citaciones | Realizado en python, no tiene las características principales que se buscan para el desarrollo en este proyecto. |
| Amun | 2014-03-21 | Diferentes módulos de vulnerabilidades | No especificado | Citado en 20 artículos diferentes en google scholar | Hecho en python, no tiene la documentación completa y se encuentra descontinuado. |
| TelnetHoney | 2016-01-20 | Telnet | No especificado | No se encontraron citaciones | No tiene documentación. Honeypot dedicado a telnet |
| Hontel | 2017-11-29 | Honeypot para telnet | No especificado | No se encontraron citaciones | Honeypot dedicado a telnet. No cumple con las características para nuestro proyecto |
| MTPot | 2017-03-20 | Especializado para mirei malware | No especificado | No se encontraron citaciones | Es un honeypot diseñado con características específicas para un virus específico, no cumple con las características para nuestro proyecto. |
| Heralding | 2018-1-21 | Especializado en caputra de credenciales | No especificado | No se encontraron citaciones | Específico para credenciales. |

Cómo es posible observar cada uno de estos honeypots difiere ampliamente del otro. Cada uno ofrece diferentes características y se enfocan en diferentes tipos de vulnerabilidades. La mayoría de estos honeypots se encuentran descontinuados y no cuentan con soporte. Esto dificulta su selección pues no es posible garantizar su mejor uso y algunas de sus características pueden estar obsoletas. Adicionalmente, fueron creados para proyectos específicos, por lo tanto, no suplen completamente los requerimientos necesarios para este proyecto. Con respecto a su nivel de interacción la mayoría no especifica qué tipo de interacción tiene haciendo difícil diferenciar si este aspecto puede afectar el proceso de obtención de información

Luego de la comparación de los diferentes honeypots, fueron seleccionados para evaluación dos de ellos, Compot y KFSensor educational. Estos dos honeypots ofrecen captura de información que es relevante para el desarrollo de este proyecto y cuentan con soporte. Compot ofrece un emulador de infraestructura de una empresa activa y atractiva para atacantes, pero, como aún se encuentra en fase de desarrollo tiene características limitadas. Para nuestro interés Compot sólo ofrece captura de información HTTP, SMTP y MODBUS, esto limitaría el alcance que se busca desarrollar con el dataset. KFSensor es un honeypot comercial por lo cual cuenta con soporte, KFSensor ofrece herramientas de monitoreo, simulación, reporte y alertas lo cual lo hace un honeypot bastante completo y cumple con todos los requerimientos de captura de información necesarias para este proyecto. Por las herramientas ofrecidas por KFSensor y la falta de otros honeypots que ofrezcan características de captura tan completas decidimos que KFSensor será el honeypot para el desarrollo del proyecto.