Luego de hacer una revisión de los honeypots server seleccionados anteriormente notamos que no satisfacen las necesidades planteadas para el proyecto porque no permitían una emulación completa del servicio web, que es nuestro principal enfoque. Al no poder emular completamente el servicio web y sus vulnerabilidades no nos permite obtener un dataset con todas las características necesarias. Al encontrar estas limitaciones iniciamos una búsqueda de un honeypot web que cumpla con las características de emulación de vulnerabilidades de aplicaciones web y tenga la capacidad de caracterizarlas.

Características deseables:

Emulación de vulnerabilidades como XSS, SQL Injection y si es posible XEE.

Tener la capacidad de clasificar un ataque a este tipo de vulnerabilidad.

Tener la posibilidad de exportar la captura del tráfico a archivo PCAP o Alguno similar que permita realizar la conversión.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre | Fecha Actualización | Vulnerabilidades | Tipo interacción | Comentarios |
| Gastopf | 4/03/2018 | Remote File Inclusion  Local File Inlcusion  HTML Injection  SQL Injection | No especificado | A pesar de que su ultimo commit es reciente el proyecto como tal no tiene actualizaciones recientes.  Queda pendiente revisar la parte de captura de trafico |
| Snare/Tanner | 9/03/2018 | Creación de clones de páginas  Falta mirar como funciona las vulnerabilidades | No especificado | Es un honeypot que tiene actualizaciones recientes, dice ser el sucesor de Gastopf.  Queda pendiente revisar cómo funciona y como se ejecuta la captura de trafico |
| Phpmyadmin\_honeypot | 3/07/2015 | Emulación de administrador de php | No especificado | Enfocado a otro tipo de vulnerabilidad |
| Nodepot | 23/08/2015 | Joomla attack (SQLInjection)  Technote 7 (Remote File Inclusion)  OpenFlash (File upload)  SQL Injection  Joomla JCE (Cross-Site Scripting) | No especificado | Falta revisar los métodos de captura de tráfico.  Posee elementos de tecnologías con vulnerabilidades |
| basic-auth-pot | 15/01/2015 | Autenticación flaws | No especificado | Enfocado en autenticación |
| Shadow Daemon | 3/02/2018 | SQL injections  XML injections  Code injections  Command injections  Cross-site scripting  Local/remote file inclusions  Backdoor access | Alta interacción | Vale la pena revisar es bastante completo. Hay que complementar con una aplicación vulnerable |
| Serveltpot | 12/05/2013 | No especificado | No especificado | Viejo, incompleto |
| Google Hack Honeypot | 07/04/2007 | Ataques mediante servidores de búsqueda | No especificado | Viejo, no se adapta a nuestro problema |
| Smart-Honeypot | 18/04/2014 | No especificado | No especificado | Falta información, parece ser muy simple |
| Bukkit Honeypot | 12/05/2011 | Bukkit | No especificado | Desarrollado para Bukkit |
| Laravel Aplication Honeypot | 9/05/2017 | Spam Prevention | No especificado | Desarrollado para prevenir spam |
| Stack-Honeypot | 30/1/2014 | Spam Prevention | No especificado | Diseñado para prevenir spam |
| EoHoneypotBundle | 26/4/2016 | Spam Prevention | No especificado | Diseñado para prevenir spam |
| ShockPot | 17/12/2015 | CVE-2014-6271. | No especificado | Exploit de bash |
| django-admin-honeypot | 7/08/2016 | Fake Django admin screen | No especificado | Diseñado para simular un login de Django |
| WebTrap | 1/1/2018 | Login Problems | No especificado | Clona páginas reales para timar a los hackers |
| honeyhttpd | 21/1/2018 | No especificado | No especificado | Captura los datos de las peticiones realizados a servidores web.  soporta python 2 y 3 |

Los honeypots web escogidos para analizar son snare/tanner y shadow daemon.