Web Application Honeypot – Open Security Summit

OWASP

The Open Web Application Security Project

Adrian Winckles

OWASP Cambridge Chapter leader

Anglia Ruskin University – Course Leader

Bio – Adrian Winckles

OWASP
The Open Web Application Security Project

- Adrian Winckles is Course Leader/Senior Lecturer for BSc(Hons) Information Security and Forensic Computing and Security Researcher at Anglia Ruskin University. He is OWASP Cambridge Chapter Leader, OWASP Europe Board Member and is involved in rebooting the Cambridge Cluster of the UK Cyber Security Forum.
- His security research programs include (in)security of software defined networks/everything (SDN/Sdx), novel network botnet detection techniques within cloud and virtual environments, distributed honeypots for threat intelligence, advanced educational techniques for teaching cybercrime investigation and virtual digital crimescene/incident simulation.
- He has successfully competed a contribution to the European FP7 English Centre of Excellence for Cybercrime training, research and education (ECENTRE). He is vice chair of the BCS Cyber Forensics Special Interest Group.

Old Project

- Old wiki entry -
  - OWASP Wiki
- Server backend removed when Ryan left Trustwave
- VM's disappeared from WASC's projects repository
- Expertise probably within ModSec Core Rule Set (CRS) Project

In the meantime

- Does anyone have the old honeypot VM’s?
- Have intern creating new probe and backend server at PoC.
- Will make backend server available to community as have some capacity in university data centre.

Project Reboot

OWASP
The Open Web Application Security Project

- Update new wiki
- Update new Github
- Design and document a Proof of Concept System/Network Architecture to act as a test bed for future experimentation.
- Develop and document a minimum of one virtual/physical honeypot device that can be deployed remotely either as a VM image, Docker container or a small factor device such as Raspberry Pi (with appropriate dummy web application)
- Install and configure a back end server to receive ModSec communications from honeypot devices. Test at least one honeypot device to communicate with the server and receive attack alarms
- Mechanism to update probe with any CRS changes
- Development of a PoC mechanism to display honeypot alarms on back end server.

Futures

- Docker based honeypot probe, small computing profile honeypot
- Provide mechanism for providing open source threat intelligence to the community.
- Provide mechanism for catching specific web vulnerabilities

Questions/Volunteers…

OWASP

The Open Web Application Security Project