Thesis Internship: Network Honeypot Framework

Auxilium Cyber Security GmbH

Thesis Goal

Auxilium Cyber Security is information security research & consultancy company mainly active in the fields of Information Security Strategies (ISO27001, NIST Cybersecurity Framework, PCI-DSS), penetration testing and threat intelligence research. We have developed internal platform to detect high profile information security threats including information on specific attack vectors.

We are currently seeking to research and develop adjustable network honeypot framework allowing to detect and analyze those attack vectors in real world. Framework should be based on modules, loading each allowing to simulate specific vulnerability and monitoring exploitation attempts. MSc thesis researcher joining our team will get a chance to utilize state-of-the art virtualization equipment as well as to measure the effectiveness of developed honeypot framework directly on the open Internet or potentially in the internal networks of large multinational enterprises.

Research Plan

1. Examine existing academic research into the topic of network honeypots frameworks with auditing (including design and effectiveness considerations), i.e.:
    a. Provos, Niels. "A Virtual Honeypot Framework." USENIX Security Symposium. Vol. 173. 2004.
    b. Provos, Niels. "Honeyd-a virtual honeypot daemon." 10th DFN-CERT Workshop, Hamburg, Germany. Vol. 2. 2003.
    c. Nazario, Jose. "PhoneyC: A Virtual Client Honeypot." LEET 9 (2009): 911-919.
    d. There are also examples of past academic thesis works on the topic:
        i. Building a Honeypot to Research Cyber-Attack Techniques by Simon Bell, University of Sussex
        ii. Improving network security with Honeypots by Christian Döring, Darmstadt University of Applied Sciences
2. Research existing open source and proprietary honeypot solutions. Auxilium would cover well-founded investments into hardware or software acquisition necessary for the research task.
3. Design and develop honeypot framework in our testing network environment. Develop alerting and auditing capabilities. Develop at least three modules to detect contemporary cyber attacks.
4. Deploy the solution in the production environment and measure the detections over pro-longed period of time. Re-design if necessary.
5. Sum up outcomes of your work as degree thesis.

Auxilium Cyber Security GmbH · Siemensstraße 23 · D-76275 Ettlingen

www.auxiliumcybersec.com · info@auxiliumcybersec.com · +49(0)7243 - 605 990 | Geschäftsführer: Markus Ganzmann · Ingo Sauer · Marc Dilger · Robert Biesinger

Amtsgericht Mannheim · HRB 722364 · USt.-IdNr.: DE300279511 · Steuer Nr.: 31190/28549

Bankverbindung: Sparkasse Karlsruhe · BIC: KARSDE66XXX · IBAN: DE88 6605 0101 0108 2192 54

Background

Expected duration of the thesis internship: 4-6 months

Study level: Master Thesis (for aspiring students also possible as Bachelor Thesis)

Applicant Profile:

- Computer science (or related engineering) education.
- Familiar with common types of vulnerabilities and misconfigurations and related exploitation techniques.
- Familiar with basics of Windows or Linux administration.
- Enthusiast in information security

Practical Information

You will be assigned with thesis research supervisor who also successfully conducted his MSc thesis research with Auxilium Cyber Security in the past. Thesis internship can be done in partially remote fashion, but periodical meetings to discuss progress are necessary. Meetings can be arranged in Ettlingen, Germany or Prague, Czech Republic.

Get in Touch

Martin Pozděna

Senior Information Security Consultant, Auxilium Cyber Security GmbH
research@auxiliumcybersec.com
+49 173 7048 649