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 (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 (or adapt existing open source solution) in our testing network environment. Develop at least three modules to detect contemporary cyber attacks (i.e. EthernalBlue). Contemporary cyber attacks will be selected cooperatively by Auxilium Cyber Security and aspiring student based on student interest, Auxilium needs and risk level of respective attacks prior the thesis internship starts. Only attacks with publicly available exploits will be considered (at least proof of concept exploits crashing the service).
4. Deploy the solution in controlled environment and measure detection efficiency of attacks artificially invoked against the honeypot. Modify exploit parameters (shellcode, return addresses, etc.) and measure whether it affects detection capabilities. Re-design honeypot if achieved detection results are insufficient.

5. (optional) Deploy the solution in the production environment (either internal network of one of the Auxilium's customers or publicly on the Internet) and measure the detections over pro-longed period of time.
6. Sum up outcomes of your work as degree thesis.

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