Secura
Possible internships assignments

INTRODUCTION

Secura is a Centre of Excellence in Digital Security. For this reason, research & development and knowledge sharing (including presentations and publications) are of essential importance to the organisation. Secura is looking for graduates who want to conduct their final internship assignment with Secura.

Secura actively looks for young talent with an HBO/WO background and preferably a technical focus (i.e. computer science, information science, cyber security, electronics, physics etc). We believe that young talent combined with the experience we already have leads to a better and safer digital future.

This document provides several ideas for internships. These ideas are not set in stone, as we would like to discuss the actual how, what, and where in person. It is also possible for you to provide us with your own ideas for possible internships. We are more than willing to see what is possible and what is not.

All our internships are in English unless stated otherwise.

INHOUD

AUTOMATIC IOT EXPLOITATION

Project Overview

Goal:	Automatic discovery and exploitation of vulnerabilities in IoT devices		
Location:	Eindhoven / Amsterdam	Timeframe:	6 months
Complexity:	High	Team:	Security Specialists
Category:	IoT / pentesting / SW	Supervisor:	Matthijs / Robin

Student Attributes

Education: WO, MSc preferably, in computer science or the cyber security field

Technical skills:
- Proven software development skills
- Affinity with the complexity and diversity of IoT devices
- Basic understanding of pentesting and exploitation

Soft skills:
- Ability to work well in an international team environment
- Good communication skills, self-organization
- Writing skills

Project Description

Within this internship you will focus on the IoT domain (various products), where you will support us to create a tool for automatic discovery and exploitation of vulnerabilities within IoT devices. You will be:

- Designing and implementing software that is capable of emulating ARM based code for IoT devices
- Using symbolic execution, taint analysis and smt solvers to automatically locate vulnerabilities
- Propose sample exploitation techniques for these found vulnerabilities.

This is a highly complex assignment; requiring experience with software development, understanding of how exploitation works and a person who is capable of doing in-depth research.

Please find here some reference material:
http://cs.ucsb.edu/~chris/research/doc/ndss16_driller.pdf
https://github.com/shellphish/rex
https://en.wikipedia.org/wiki/2016_Cyber_Grand_Challenge
https://github.com/CyberGrandChallenge
http://www.unicorn-engine.org/
https://triton.quarkslab.com/
http://angr.io/

PASSWORD ANALYSIS 2.0

Project Overview

Goal:	Work the next version of our password analysis tool		
Location:	Eindhoven	Timeframe:	4-6 months
Complexity:	Medium	Team:	Security Specialists
Category:	Password cracking	Supervisor:	Edwin

Student Attributes

Education: BSc / MSc

Technical skills:

- Programming (Python, Powershell, Bash).
- Data structures, Data visualization
- Cryptanalysis
- System administration

Soft skills:

- Project management
- Product acquisition process
- Good communication skills, self-organization
- Writing skills

Project Description

Within Secura we perform brute-force and dictionary attacks on a regular basis. This project takes these activities to the next level by automating password analysis and creating a distributed and scalable solution which is accessible via the internal network.

Goals in this project are:

- Creating a secure way of accessing the system and transferring files from our internal network.
- Automate the password cracking process with customizable flags for cracking and an added option of generating a report.
- Implement a worker queue based on weight of the assignments with feedback to the user.

Challenges will be in the following areas:

- Product acquisition and implementation process.
- Secure communication and access control with the system.
- Creating a design that is scalable and distributed.
- Importing and interpretation of data from files with a different format.
- Providing the users with feedback of their jobs.

DESIGNING + SETTING UP A FORENSIC NETWORK

Project Overview

Goal:	Design a forensic network		
Location:	Eindhoven/Amsterdam	Timeframe:	4-6 months
Complexity:	High	Team:	Security Specialists
Category:	Forensics	Supervisor:	Guus

Student Attributes

Education: HBO or University in a technical field of study (Computer Science, informatics, Engineering, Forensics)

Technical skills:

- Affinity with digital forensics and security
- Knowledge of digital forensic procedures and way of working
- Is able to design a network architecture that will be under heavy load

Soft skills:

- Ability to work well in an international team environment
- Good communication skills, self-organization
- Writing skills

Project Description

Forensic investigators handle sensitive data during their investigations. Therefore, the data should be investigated in a safe and secure environment. The network infrastructure of Secura should be able to support this endeavor. Forensic networks need to be able to handle certain requirements while supporting the forensic investigation workflow. The next couple of paragraphs will cover this in greater detail.

The forensic investigation workflow has been defined by NIST in 2006 and consists of the following steps:

- Collection - identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.
- Examination - forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.
- Analysis - analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- Reporting - reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions

need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process

A forensic network should be able to support this workflow without any problem if an organization wants to be successful. A list of requirements might look similar to the list displayed below, note that this is not a complete list by any means.

- The network should be able to handle a large amount of throughput, courtesy of various data sources during an investigation.
- The network should be able to handle different data sources, hard disks, flash storage, mobile devices, packet captures, etc.
- All activity on the network should be audited, the logs available for inspection at any time within secure Secura premises.
- Maintaining standardized base lines and configuration of investigative equipment.
- etc...

The goal for this internship is to make a design for a forensic network that can be readily implemented by Secura.

TESTING FORENSIC TOOLING

Project Overview

Goal:	Test tools on a variety of forensically acquired sources to confirm its suitability to be used in digital forensic investigations.		
Location:	Eindhoven	Timeframe:	6 months
Complexity:	High	Team:	Security Specialists
Category:	Forensics	Supervisor:	Guus

Student Attributes

Education: HBO or University in a technical field of study (Computer Science, informatics, , Forensics)

Technical skills:

- Affinity with digital forensics
- Knowledge of digital forensic procedures and way of working
- Analytical thinking

Soft skills:

- Ability to work well in an international team environment
- Good communication skills, self-organization
- Writing skills
- Works in a precise and exact manner

Project Description

A forensic investigator uses a variety of tools during an investigation. While the integrity of industry mainstays like EnCase and FTK are pretty much guaranteed, the same can't be said for many other tools which might be needed in the course of an investigation. Validation of tools used during an investigation is needed to ensure its suitability and reliability in court proceedings. Further testing includes common scenarios in digital forensics such as log files and analysis on common file types.

Any tools used during investigations need to be able to stand up to two interrelated principles, *repeatability* and *reproducibility*. The *repeatability* principle refers to obtaining the same results when using the same method on identical test items in the same laboratory by the same operator using the same equipment within short intervals of time. The *reproducibility* principle refers to obtaining the same results being obtained when using the same method on identical test items in different laboratories with different operators utilizing different equipment.

These principles form the foundation of the Daubert principle. The Daubert principle is used in legal circles to establish the reliability of scientific methods. It uses five questions in order to make a determination:

1. Has the method in question undergone empirical testing?
2. Has the method been subjected to peer review?
3. Does the method have any known or potential error rate?
4. Do standards exist for the control of the technique's operation?
5. Has the method received general acceptance in the relevant scientific community?

The scientific journal, Digital Investigation, dedicated to digital forensics and incident response contains many findings which might be of interest to Secura. The articles can be used to acquaint an organization with digital forensics and build an initial knowledge base.

Recent articles, suitable for inclusion in the knowledge base include:

- Forensic analysis of Telegram Messenger on Android smartphones
- Live acquisition of main memory data from Android smartphones and smartwatches
- Decoding the APFS file system

The goal of the internship is to create a ready to use knowledge base covering common scenarios, validated by in-house tests and the wider digital forensics community. The knowledge base would cover how to perform investigations on forensic artifacts, the validated tools, as well possible avenues and procedures on further testing.