Project Proposal

Student: Simon Bell

Project supervisor: Martin Berger

Working title: Building a honeypot to research cyber-attack techniques

Aims

The aim of this project is to build a low-interaction, production SSH honeypot. This honeypot will be deployed on a public server to research cyber-attack techniques.

My primary motivation for undertaking this project is my fascination with the modules: computer networks and operating systems - in particular the security parts of these modules. I'm keen to explore cyber-attack techniques and computer security vulnerabilities in more detail through my own project and research.

Primary Objectives

Design and build SSH honeypot

I will be using the programming language C; since this is the language which the SSH daemon is built in. By using C the aim is to make the honeypot behave as similarly as possible to a real SSH daemon and therefore appear convincing to an attacker.

This will involve analysing the timings of operations, and outputs of commands. I will only deploy a limited set of shell commands - the most common commands used by an attacker - to allow an attack to take place.

Test honeypot

I want to ensure the honeypot is as convincing as possible in order to encourage attackers. Since I'm building the honeypot in C I will also need to ensure it is safe and does not create a vulnerability to the system. I will conduct mock attacks on the honeypot to test its robustness along with a series of automated tests.

Deploy to public server

I will deploy the working SSH honeypot to an Amazon Elastic Compute Cloud (EC2) public server. The aim here is to attract attention to the server in order to be able to analyse cyber-attacks.

Extensions

- Create a number of websites/blogs focusing on particular topics and run honeypot on this server to analyse attracted attacks
- Allow attackers to upload code and run/analyse this uploaded code in a safe environment for analysis
- Explore other honeypots such as open mail relay

Relevance

This project relates heavily to the Computer Science degree. At its core it uses knowledge and understanding of programming, networks and security. This project also relates to malware and operating systems.

Resources required

This project will require a public server to run the working honeypot on. I will be using an Amazon Elastic Compute Cloud server for this.

Interim log

Previous meetings during June/July/August 2013

Met to discuss project ideas, areas to research, language implementation.

Thursday 26th September 2013

Met with supervisor to discuss progress on project. Agreed to produce a working C server which allows basic connection/login.

Bibliography

Cavallaro, L (2013) 'Malicious Software and its Underground Economy: Two Sides to Every Story'. Coursera.org [online]. Available from: https://www.coursera.org/course/malsoftware (accessed June 2013)

Timetable

	Monday	Tuesday	Wednesday	Thursday	Friday
09:00 - 10:00		Final Year Project	Final Year Project		
10:00 - 11:00		🟧	🟧		
11:00 - 12:00		🟧	🟧	Comparative Programming Lecture	
12:00 - 13:00		🟧	🟧	Comparative Programming Lecture	
13:00 - 14:00	Web Computing Lecture				
14:00 - 15:00	Web Computing Lecture	🟧	🟧	HCI Seminar	Comparative Programming Lab
15:00 - 16:00	Web Computing Lab	🟧	🟧		
16:00 - 17:00		🟧	🟧		
17:00 - 18:00	HCI Lecture	🟧	🟧		

Key:	Lectures / labs: 8 hours	Final year project: 16 hours