Initial Plan - Analysis and Visualisation of Access Attempts on a Honeypot Server

Project Description

This project would involve the creation of a modified SSH server variant used as a 'honeypot' server to capture and analyse intrusion attempts of different varieties. The modified SSH server would be run on a number of different Raspberry Pi's and modified from the open source version currently available, each Pi would be used to analyse a different type of intrusion attempt.

The adapted version of the SSH server would have the ability to masquerade as any version of an SSH server and would appear like a normal unmodified server to a would-be attacker. This would then be used to remotely log access attempts such as passwords used in brute-force attacks and to see if any exploits were attempted to be levied against the server by looking for the signatures of selected attacks using knowledge gained from their CVE entries.

This information collected can then be stored and analysed for the purpose of showing what passwords are regularly tried on public facing servers, what versions are most vulnerable to exploit attempts and metadata about the would-be attackers such as originating country of attack or proxy location.

I will also be developing a web interface to visualise this collected information in a both historical and real-time view. The web GUI should be able to show data being collected in real-time with passwords and access attempts being shown in a user-friendly way, as well as being to show historical trends using graphs and figures.

Project Aims and Objectives

- To modify existing open source code for an SSH server to include remote logging
- To create a database system to allow the storage of logged data including passwords attempts and other metadata
- Create a web GUI that shows historical and real-time data in a suitable format
- Develop a method of detecting a selected exploit attempt
- Use analysis methods to discover commonly used passwords for SSH brute force attacks
- Attempt to show what the most targeted vulnerable versions of SSH are
- Store as much information as possible about attempted SSH sessions for further analysis
- Decouple the server side logging with the database and GUI where possible
- Use commonly supported formats for the GUI such as REST APIs and JSON for data transfer
- Make the honeypot server not differ to a normal SSH server to a would-be attacker
- Maintain the security of the Raspberry Pi's at all times
- Create readable and maintainable code
- Use configuration options for the server to allow for choosing of modes including type of logging and the ability to disable logging entirely
- To use my findings to provide advice on improving the security of publicly accessible SSH servers

Work Plan

Week 1 (30th Jan) – Obtain and understand SSH server code from open-source communities and discuss hardware with Inserv

Week 2 (6th Feb) – Design stage and prototype basic communication from server

Week 3 (13th Feb) – Create database system back end and finalise basic communication

Week 4 (20th Feb) – **Progress meeting with project supervisor**, discussing any problems/feedback, Building on communication and storage functionality, should have a basic working prototype at this stage.

Week 5 (27th Feb) – Finalise storage and analysis information back-end, **Deliverable:** SSH server storing password attempts to Mongo database

Week 6 (6th Mar) – Develop web GUI framework showing data analysis and start writing report

Week 7 (13th Mar) – Further web development and reporting on design choices/introduction

Week 8 (20th Mar) – Web development and 'catch-up' time

Week 9 (27th Mar) – Design and implement feature to detect exploitation attempts, **Deliverable:** Fully working honey pot server implementation

Week 10 (3rd Apr) – Finish web GUI with statistics and analytics, **Deliverable:** Web GUI working from database

Week 11 (10th Apr) – Report writing & **progress meeting with project supervisor**

Week 12 (17th Apr) – Report writing

Week 13 (24th Apr) – Report writing

Week 14 (1st May – 5th May) – Finish Report **Deliverable: Final report**

Throughout the process I will be taking detailed notes to discuss the choices I made and why I made them including any problems I face and how I overcome them.

Ethical Issues

My main ethical concern with this project is the potential for the devices used as honeypots to be hijacked for nefarious activities. While I will be putting security considerations as a high priority, it is not possible to guarantee absolute security for the devices being used in the project as they will be targeted by hackers or other groups. This leads to the concern that the devices could be hijacked and used for illegal purposes from the University network. To combat this I will be checking the devices regularly for any security flaws or unusual networking activity and any outgoing connections other than my own will be treated as unusual and the appropriate action be taken.

I have also discussed ethical considerations with George Theodorakopoulos, who is part of the university's research ethics group at the beginning of this project and he has confirmed that it is within the ethical guidelines required for a final year project.