Initial Plan

Visualising Malicious Network Activity

Author: Aled Owain Mason
Student no: 1130538
Supervisor: Prof. Omer F. Rana
Moderator: Mr Michael Daley
Module: CM3203 - One Semester Individual Project
Credits: 40

Project Description

Recent advances in technology have been rapid and people all around the world have felt its effects. The development of the World Wide Web has allowed instant information retrieval for almost every subject and a way to communicate to almost everyone around the world. With these developments however, computer systems have been susceptible to malicious attacks through vulnerabilities in their design and/or implementation. These attacks are all made possible by computer networks; namely the Internet. As a result, network administrators are expected to mitigate these threats and analyse their behaviour.

This project will aim to study these attacks by capturing and analysing malicious network activity. Specifically I aim to build a software environment, which is capable of visualising pre-collected network data. It should then be possible to further develop this software to visualise network data in real-time. From this, network administrators will be better equipped to quickly analyse malicious attacks sent to their networks.

Initially this software will visualise information collected by Cardiff University Information Services (INSRV), so the program can analyse more *interesting* network traffic. In week 1, I met with Damian Southard from INSRV who explained that there are many different sources for capturing such network data including Firewalls, Intrusion Detection Systems and Honeypots. Each of these allow different capturing methods which produce different output formats, each of which are useful for a variety of purposes. Another important aspect to consider is the size of the data collected on a particular date/ time to gain an accurate and varied perspective of network activity.

Initially I plan on using IDS logs which contain low level pcap data (raw network traffic) taken from a 24 hour capture. With this information it should be possible to extract the source and intended destination of a malicious attack, what vulnerability the attack was targeting, etc. I should also be able to predict the potential impact of the attack itself. Using IDS capture logs and pcap data, it should also be possible to link a malicious attack to the Common Vulnerabilities and Exposures database.

Aims and Objectives

Create a software environment to visualise malicious network activity.

- Learn how to identify malicious network packets.
- Discover common types of attack launched towards INSRV networks.
- Research what kind of visual data will be useful for a network administrator for security issues.
- Build a software program to produce various graphs/ charts visualising malicious attacks from pre-collected network data.
- Further develop the software program to analyse real-time network activity and link entities to the CVE database.

Work Plan

Week 1

- Write the initial plan.
- Meet with Damian Southard from INSRV to discuss data sources and formats.

Week 2

- Write an introduction and background to the project.
- Receive and analyse data provided by INSRV.
- Research potential tools to aid my project goals.

Week 3

- Write the approach to the project.
- Begin simple querying to the data, making note on how to extract useful information.
- Identify specifications and start designing the visualisation software for use with pre-collected INSRV data.

Week 4

- Meet with Supervisor to check progress and make any necessary modifications to the project.
- Continue designing visualisation software.

Week 5-7

- Begin implementation of visualisation software.

Week 8-10

- Meet with Supervisor to check progress and make any necessary modifications to the project (Week 8).
- Continue implementation of visualisation software to include real-time analysis of malicious network activity and CVE database linking.

Week 11

- Evaluate and write the results to the project.

Easter Holiday Week 1

- Write possible future work to the project.
- Write a conclusion to the project.

Easter Holiday Week 2

- Continue writing the conclusion.
- Write reflections on learning.

Easter Holiday Week 3

- Complete any missing contents.
- Proof reading.