Development and Implementation of a Honeynet on a University Owned Subnet

Erin L. Johnson, John M. Koenig, Dr. Paul Wagner (Faculty Mentor)
{johnsone, koenigjm, wagnerpj} @ uwec.edu
Computer Science Department – University of Wisconsin Eau Claire

Background

In network security there are several ways to gain information about attacks and program vulnerabilities. One way to do this is to install computers whose sole purpose is to be attacked and then passively log all activity on these computers. A honeynet is a technology that provides this functionality. From honeynet data we can study attackers' modus operandi and motives directly, allowing for the development of better security tools.

Overview

The focus of our research project is to implement a honeynet at the University of Wisconsin Eau Claire (UWEC) according to the stipulations set forth by the Honeynet Research Alliance (HRA) while operating with limited resources. Our overall goal is to profile malicious activity in a class C subnet and use this data to fill a demographic gap as well as act as a base for future research.

What is a Honeynet?

A honeynet is a network of unsecured computers (called honeypots) whose sole purpose is to be attacked. All network activity on the honeynet is passively logged. Because there is no viable reason for anyone to be connecting to these computers, all activity can be reasonably considered malicious. To gather this activity as well as mitigate risk, there have been several tools developed, such as honeywall, which is developed by the Honeynet Research Alliance (HRA). The honeywall is between the Internet and the honeynet and fulfils all of the implementation requirement set forth by the HRA.

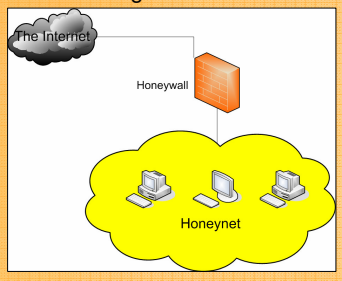

Fig 1. A Honeynet Using Honeywall

Honeynet Research Alliance

For our honeynet we followed the implementation requirements set forth by the Honeynet Research Alliance (HRA). HRA brings together other Honeynet Projects and consists of roughly 20 members world wide. Their goal is to develop honeypot/net related technologies and share data. As of right now there are no alliance members from a Tier 2 University such as UWEC.

Implementation Requirements

1. Data Control: Must be passive and must be able to modify or deny malicious packets.
2. Data Capture: Log network traffic and honeypot activity
3. Data Analysis: Must have a means to extract and analyze captured data
4. Data Collection: Must have a secure location to store data

Our Honeynet

Our original goal was to mimic the UWEC network as closely as possible while staying cost effective. To keep costs down we decided to implement our honeypots as virtual systems. However, due to several software conflicts our honeypots are Ubuntu Edgy installations rather than Windows XP.

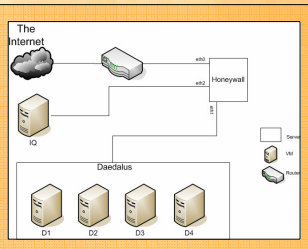

Fig 2. Our Honeynet

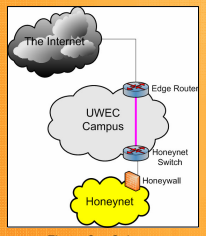

Fig 3. Our Subnet

Our Network

In addition to the data control measures provided by honeywall, network traffic generated from our subnet cannot reach the primary UWEC network. The only traffic from the primary UWEC network that can reach our subnet must be using SSL or SSH. Also, all honeynet traffic must pass though a switch that systems administrators can shut down in an emergency.

Acknowledgements

We would like to thank our research advisor, Dr. Paul Wagner, as well as Jason Wudi, Tom Paine, and Eric Stevens for their support.

Funding provided by the Office of Research and Sponsored Programs and Differential Tuition.