

Research in Honeypot Technologies
Karl Schuttler (E00921961)
Eastern Michigan University College of Technology

1. Introduction

The proposed research project serves to act as a practical, real-world lab on the use of existing honeypot and Intrusion Detection System (IDS) softwares.

Honeypots are traps set to detect, deflect, or counteract attempts at unauthorized use of information systems. These consist of a computer or multiple computers that appear to be part of a larger network, but are actually isolated and monitored. IDS softwares serve in this situation as a tool to transparently monitor the information communicated to the honeypot, and log all activity.

By actively viewing a research honeypot, the researcher will gather information about the tactics and tools used by computer criminals. It will serve as a window to view the illicit activities present on the internet, in conjunction with providing real-world training on the use of an Intrusion Detection System.

2. Description of Proposed Research

This project is to be conducted through the use of two physical servers and a segment of public IP space isolated from EMU's internal network. The focus of this project is to gain real world education on the use of the Snort intrusion detection system, and to gain further insight into the methods and tools used by hackers. It will be monitored throughout the duration of the school year, or until the use of the system is no longer providing new knowledge or expertise.

The primary server will run honeyd, a virtual honeypot software that can be configured to respond to system probes in a variety of different manners in order to imitate various computer system profiles. It will use arpd to listen for ARP requests and answer for unallocated IP addresses, giving it the ability to make unused IP addresses appear as valid production servers. This function can also be provided by setting the virtual host IP addresses statically, if given static IP addresses, or over DHCP. DHCP has the disadvantage of resetting IP addresses each time the honeyd service is reset, making it difficult to correlate log information. In preparation for the possibility of a hole in the honeyd software, all instances of honeyd will be ran in a chroot to remove the threat of escaping and overrunning the server itself.

The secondary server will be either connected in line or via a span port, running the Snort intrusion detection system. Snort will allow for an improved logging system in lieu of honeyd's poor log management, and in addition give the system a variety of front ends to watch interactions with the system in real time. It will use the Basic Analysis and Security Engine (BASE) to provide a web based front end, although other front end systems that interoperate with Snort will be experimented with to gain a greater familiarity with the IDS. This server will also run sshd as its method of remote communication.

3. Research Resources

This project will require two 1.0 Ghz class computers with a minimum of 20gb disk space and an isolated segment of public IP addresses. If it is available, a class C subnet in the DMZ with static IP assignment would allow for a great variation in the amount of virtual hosts so that experimentation with scale would be possible. If required, the servers and a consumer grade router can be supplied by the researcher.

4. Personnel

As project head, Karl Schuttler will be the only participant involved in the project. The details and outcomes of this project may be shared and collaborated with other Information Assurance staff and students, but the project is only to be operated by Mr. Schuttler.

Karl Schuttler is a Sophomore undergraduate student seeking a Bachelor's degree in Information Assurance from Eastern Michigan University's College of Technology.