CALIFORNIA STATE SCIENCE FAIR
2009 PROJECT SUMMARY

Name(s)

Ryan Dempsey; John Templeman

Project Number

S1604

Project Title

Honey Cluster Computing vs. Distributed Denial of Service Attacks

Abstract

Objectives/Goals

The objective of the project is to show the effect of the utilization of a single system image (SSI) cluster computing platform as a centralized management, action, and deployment point for distributed honeypot systems on the number of captured, repelled, and countered hacker attacks, in order to better enhance computer network security.

Methods/Materials

Four computers were set up as a simulated DDoS attack group, four computers were set up as the Honey Cluster, and two computers were set up as the Nmap Scanner Cluster. The four DDoS computers first attacked the control group, made up of the same computers as the Honey Cluster. After this control attack, the DDoS computers attacked the experimental Honey Cluster computers. The data collected from the attacks was the ratio of outgoing to incoming packets, measured on the control group computers and the Honey Cluster.

Results

This was chosen because DDoS attacks are dangerous in nature, potentially affecting hundreds of computers on a given network. After a simulated DDoS attack on the Honey Cluster, the Honey Cluster#s response to the attack was shown to be a statistically significant DDoS countermeasure relative to the control computer systems. The LaBrea Honey Cluster enacted a reactive-defense counter to the DDoS attack, fully repelling and redirecting 160% of the packet flood back to the DDoS group. When the control computer systems were attacked by way of a simulated DDoS, the control computers sent 0% of the original attack packets back to the DDoS group. The ultimate result of the DDoS redirection was a total stoppage of services and exploits in the simulated DDoS Group.

Conclusions/Discussion

By analyzing the results, experimentation has shown that cluster computing in regards to honeypot technology, specifically known as a Honey Cluster, can provide statistically significant protection against DDoS attacks. Hackers have been statistically shown to be dangerous people, with dangerous motives and dangerous intentions. Protecting against hackers by means of Honey Cluster technology is the main goal of this project. This endeavor has shown the potential to provide greater levels of security to the public. The success of this endeavor shows that defense against such prolific and prevalent threats as DDoS attacks is possible, probable, and ultimately achievable.

Summary Statement

This project is about the enhancement of computer and network security through the marriage of honeypots (an emerging security technology) and compute clusters in such a way that provides the end user a safer, more secure computer network.

Help Received

Recieved a donation of ten computers from the ZGallerie, Inc. IT Department - this was made possible by Mr. Howard Kolodny, the Director of the IT Department for ZGallerie; Mr. Lindbergh Atkins of CAMS High School helped the project through his donation of hard drives.