Abstract

Self-propagating malware, such as worms, have prompted cyber attacks that compromise regular computer systems via exploiting memory-related vulnerabilities which present threats to computer networks. A new generation worm could infect millions of hosts in just a few minutes, making on time human intrusion impossible. The new worms are spread over the network on regular basis and the computer systems and network vulnerabilities are growing enormously. Here we also facing the problem of automatically and reliably detecting previously unknown attacks which are known as zero-day attack. In this paper, I have described the use of the Honeycomb to detect Zero-day attack in Virtualized network. A method to automatically generate signatures using the proposed detection system is presented. The attack signatures are detected and scanned through the system. Honeycomb is a host-based intrusion detection system that automatically creates signatures. It uses a honeypot to capture malicious traffic targeting dark space, and then applies the Longest Common Substring (LCS) algorithm on the packet content of a number of connections going to the same services. The computed substring
Detecting Zero-Day Attack Signatures using Honeycomb in a Virtualized Network

is used as candidate worm signature. Honeycomb is well suited for extracting string signatures for automated updates to a firewall.

Reference

- C. Xenakis a, C. Panos b, I. Stavrakakis b: A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, elsevier, computers & security 30 (2011) 63-80
- Dr I. Muttik, McAfee Labs, UK: ZERO-DAY MALWARE, Virus bulletin conference September 2010.

Index Terms

Computer Science  Security
Key words

Zero-Day attack
Honeycomb
Malware
Automatic Signature Generation