SIGNATURE BASED INTRUSION DETECTION AND PREVENTION SYSTEM

A dissertation submitted to the

Computer Science and Technology Degree Program,

Uva Wellassa University

in partial fulfillment of the requirements for the award of the

Degree of Bachelor of Science

By

GUNASEKARA ARACHCHILAGE HARSHA LAKMAL

Registration Number: UWU/CST/09/0022

Computer Science and Technology Degree Program

Uva Wellassa University, Sri Lanka

October 2013

ABSTRACT

When securing a computer or a network from attacks (unauthorized access), most important things is to be aware of the vulnerabilities of computers in a network, be aware of attacks and how to remove or prevent them. A honeypot is a closely monitored network decoy serving several purposes: it can distract adversaries from more valuable machines on a network, provide early warning about new attack and exploitation trends, or allow in-depth examination of adversaries during and after exploitation of a honeypot.

Signature based Intrusion Detection System (IDS) has a weakness in not being able to detect unknown attacks until new signatures are created for the attack manually. This project describes an automatic rule generating system for IDS using Honeypot and honeyd. TheHoneyd is a framework for virtual honeypots that simulates virtual computer systems at the network level. The simulated computer systems appear to run on unallocated network addresses. To deceive network fingerprinting tools, Honeyd simulates the networking stack of different operating systems and can provide arbitrary routing topologies and services for an arbitrary number of virtual systems. Because deploying a physical honeypot is often time intensive and expensive as different operating systems requires specialized hardware and every honeypot requires its own physical system.

This is a good and essential part of the network security environment which enables detection of suspicious packets and attacks. In this project authors focus is to create auto generated ACL for any intruder who comes to the Honeypot initially. This will prevent the intruder from hacking the system. And also web based application to review and analyze the statistics in the environment. Automatic generation of rules reduces the chance of the IDS not detecting an intrusion attempt it also reduces the workload of network administrator. Most importantly it enhances the detection ability of the IDS. When this system is used IDS will be able to quickly identify new attacks.