Computer Science & Engineering Department

SOA paper crunch

Attack Evaluation Framework based on Netfilter

Project Proposal, Operating Systems - Practical, Autumn 2011

Index terms: security, networking
Keywords: attack, netfilter
Team size: 2

1 Project Description

Netfilter is a framework that provides hooks in the Linux kernel for intercepting and altering network packets.

This project implements a framework for evaluating and classifying malicious attacks. The framework consists of a loadable kernel module that gathers information about network traffic using Netfilter hooks and a userspace application that analyses this traffic in order to classify and evaluate attacks.

2 Objectives

This project aims to implement a software application that will meet the following requirements:

- The kernel module should capture all network traffic
- The kernel module should store a log file with all suspicious events
- The userspace application should be able to parse and analyze the information stored in the log file
- The application should use the information to classify and evaluate malicious attacks
- Human-readable information should be provided to the security expert for further analysis
- A configuration file should be used as a method to configure the framework

3 Bibliography

[1] Writing Loadable Kernel Modules using netfilter hooks, http://fcns.eu/2010/02/netfilter-hooks/

[2] P. Kabiri and A. A. Ghorbani, "Research on Intrusion Detection and Response : A Survey," International Journal, vol. 1, no. 2, pp. 84-102, 2005.

4 Prerequisites

Networking, security, kernel programming.