

CONTENTS

| | | |
|------------|--------------------------------------------------------------------------|----|
| Chapter 01 | INTRODUCTION | 1 |
| | 1.1 Problem Definition | 2 |
| Chapter 02 | AN OVERVIEW OF INTERNET WORMS | 3 |
| | 2.1 Categorization of Internet Worms | 4 |
| | 2.2 A Brief Discussion on Some Existing Internet Worms | 7 |
| | 2.3 Detail Study of Win32/Blaster Worm | 9 |
| Chapter 03 | Vulnerability | 13 |
| | 3.1 Example Vulnerabilities | 14 |
| Chapter 04 | Defense mechanism | 20 |
| | 4.1 Anomaly-Based Defense | 20 |
| | 4.2 Signature Based | 22 |
| Chapter 05 | Overview of Signature based protection and filtering mechanisms | 27 |
| Chapter 06 | Implementation of filtering engine | 42 |
| | 6.1 Loadable Linux Kernel Modules (LKM) | 42 |
| | 6.2 Filtering engine using netfilter | 44 |
| | 6.3 A Brief discussion on the development of the filtering engine module | 45 |
| | 6.4 Deploying RPC DCOM Vulnerability Signature in the Filtering Engine | 48 |
| | 6.5 Deploying SQL SERVER Resolution Vulnerability Signature | 55 |
| | 6.6 Network Architecture for Deploying the Filtering Engine | 62 |
| Chapter 07 | Network setup and Results | 64 |
| Chapter 08 | Conclusions & Future Work | 72 |
| References | | 74 |
| Appendix A | An overview of VMWARE | 78 |
| Appendix B | An overview of METASPLOIT | 79 |
| Appendix C | An overview of WIRESHARK | 80 |