

---

# CONTENTS

<b>Chapter 1 Introduction of Internet Worms .....</b>	<b>1</b>
1.1 What Is Malware .....	1
1.2 Internet Worms .....	2
<b>Chapter 2 Formal Definition of the Problem .....</b>	<b>8</b>
<b>Chapter 3 Study of Some Vulnerabilities and Worms .....</b>	<b>10</b>
3.1 Common Vulnerabilities Exploited by Worms .....	10
3.2 Slammer Worm Analysis .....	14
<b>Chapter 4 Internet Worm Detection mechanism .....</b>	<b>27</b>
4.1 An Overview of Existing Work .....	27
4.2 Classification of Detection Mechanisms .....	31
4.2.1 Anomaly based .....	31
4.2.2 Signature based Detection .....	31
<b>Chapter 5 Packet Filtering Mechanisms .....</b>	<b>33</b>
5.1 Introduction .....	33
5.2 Requirements for deployment of Protocol Level Signatures .....	33
5.3 Survey of different approaches .....	34
5.3.1 Networking ACL .....	34
5.3.2 Cisco IOS IPS .....	39
5.3.3 IPCop .....	41
5.3.4 SNORT .....	42
5.3.5 Iptables .....	47
5.3.6 Netfilter .....	49

---

---

<b>Chapter 6 Implementation using Netfilter .....</b>	<b>52</b>
6.1 Generic Algorithm for Packet Filtering .....	52
6.2 Target Network Architecture .....	54
6.3 Target Vulnerabilities .....	55
6.4 SQL Server Resolution Service – Module .....	56
6.4.1 Protocol Specification .....	56
6.4.2 Protocol level Vulnerability Signature to be deployed .....	60
6.4.3 Algorithm .....	60
6.5 RPC-DCOM – module .....	62
6.5.1 Protocol level Vulnerability Signature to be deployed .....	62
6.5.2 Protocol Specification – DCE RPC .....	63
6.5.3 Protocol Specification – REMACT .....	67
6.5.4 Algorithm .....	67
<b>Chapter 7 Testing Setup &amp; Results .....</b>	<b>69</b>
7.1 Platform Used .....	69
7.2 Network Setup using VMware .....	69
7.3 Attacks Used .....	70
7.3.1 Metasploit .....	70
7.3.2 Slammer variant .....	71
7.3.3 By injecting a captured (by CERT Team) attack packet .....	71
7.4 Normal Request .....	72
7.5 Results .....	72
<b>Chapter 8 Conclusions and Future Work .....</b>	<b>73</b>
<b>References .....</b>	<b>75</b>

---