DETECTION OF DENIAL OF SERVICE (DoS) ATTACKS IN LOCAL AREA NETWORKS BASED ON OUTGOING PACKETS

MEHDI EBADY MANAA

UNIVERSITY UTARA MALAYSIA
2012
Detection of Denial of Service (Dos) Attacks in Local Area Networks Based on Outgoing Packets

A project submitted to Dean of Awang Had Salleh Graduate School in partial fulfillment of the requirement for the degree

Master of Science of Information Technology

Universiti Utara Malaysia

By

MEHDI EBADY MANAA

© Mehdi, 2012
PERMISSION TO USE

In presenting this project of the requirements for a Master of Science in Information Technology (MSc. IT) from Universiti Utara Malaysia, I agree that the University library may make it freely available for inspection. I further agree that permission for copying of this project paper in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in their absence, by the Dean Awang Had Salleh Graduate School. It is understood that any copying or publication or use of this project or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project paper.

Request for permission to copy or make other use of materials in this project, in whole or in part, should be addressed to:

Dean Awang Had Salleh Graduate School
College of Arts And Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman
Malaysia
Denial of Service (DoS) is a security threat which compromises the confidentiality of information stored in Local Area Networks (LANs) due to unauthorized access by spoofed IP addresses. DoS is harmful to LANs as the flooding of packets may delay other users from accessing the server and in severe cases, the server may need to be shut down, wasting valuable resources, especially in critical real-time services such as in e-commerce and the medical field. The objective of this project is to propose a new DoS detection system to protect organizations from unauthenticated access to important information which may jeopardize the confidentiality, privacy and integrity of information in Local Area Networks. The new DoS detection system monitors the traffic flow of packets and filters the packets based on their IP addresses to determine whether they are genuine requests for network services or DoS attacks.

Results obtained demonstrate that the detection accuracy of the new DoS detection system was in good agreement with the detection accuracy from the network protocol analyzer, Wireshark. For high-rate DoS attacks, the accuracy was 100% whereas for low-rate DoS attacks, the accuracy was 67%.
ACKNOWLEDGEMENTS

First and foremost, I would like to thank our GOD “Allah”, the most gracious and the most merciful, for having made everything possible by giving me strength, confidence, and courage to accomplish this work.

I wish to express my sincere gratitude to Dr. Angela Amphawan for her guidance and direction in this work. She gave me many interesting, valuable and sincere feedbacks throughout her supervision. I greatly benefited from her detailed comments and insights that helped me clarify ideas in “Detection of Denial of Service Attacks in Local Area Networks based on Outgoing Packets”.

I sincerely thank to my evaluator Dr. Ahmad Suki Che Mohamad Arif, and other committee members, for graciously reviewing this work and giving valuable suggestion and comments on my work.

I would also like to say a big thanks all UUM lecturers and staff members at the School of Computing who were kind enough to give me their precious time and assistance, without which I would not have been able to complete this Masters Project.

I am indebted and thankful to the Chancellor of University Utara Malaysia who referred me to valuable e-recourses at the Sultanah Bahiyah Library.

I wish to thank the Ministry of Higher Education of Iraq for the financial support awarded to me.

Last but not least, extreme thanks are reserved for the last. Words cannot express my gratitude to my family, especially my sympathetic, compassionate and beloved parents, my dear brothers Ahmed, Ali, Hassan, Hussain, Mohammed and Mohmoud, my sister, my faithful wife, and my four daughters, Benin, Khawther, Fatima and Abrar. Words cannot describe their constant love, care, concern, patience, and direction in every aspect of my life throughout the two years of my study abroad. I’m forever thankful, grateful, and indebted to them. May Allah bless them! I dedicate the accomplishment of this project to my beloved father, my affectionate mother, and to the twin of my spirit, my wife.

Thank you UUM.

MEHDI EBADY MANAA
# TABLE OF CONTENTS

PERMISSION TO USE ................................................................................................. I
ABSTRACT .................................................................................................................. II
ACKNOWLEDGEMENTS ............................................................................................ III
TABLE OF CONTENTS ............................................................................................... IV
LIST OF TABLES .......................................................................................................... VII
LIST OF FIGURES ....................................................................................................... VIII
LIST OF APPENDIXES ............................................................................................... VIII
LIST OF ABBREVIATION ............................................................................................ XI

CHAPTER ONE: INTRODUCTION

1. Introduction ............................................................................................................. 1
1.1 Research Landscape and Preliminary Concepts ..................................................... 4
  1.1.1 Local Area Network (LAN) ............................................................................. 5
  1.1.2 Network Services ......................................................................................... 7
  1.1.3 Network Threats ........................................................................................... 8
  1.1.4 Denial of Service (DoS) ................................................................................ 9
1.2 Motivation of the Research .................................................................................. 12
1.3 Problem Statement ............................................................................................. 14
1.4 Research Questions ............................................................................................. 15
1.5 Research Objectives ........................................................................................... 15
1.6 Research Scope .................................................................................................. 16
1.7 Significance of Research .................................................................................... 16
1.8 Structure of the Report ....................................................................................... 17
1.9 Summary ............................................................................................................. 18

CHAPTER TWO: LITERATURE REVIEW

2. Introduction ............................................................................................................. 19
2.1 The Concept of Denial of Service (DoS) Attack .................................................... 19
2.2 IP- Spoofing based TCP/IP .................................................................................. 20
2.3 TCP/ IP Packet Structure ................................................................................... 21
2.4 Previous Work on DoS Methods ......................................................................... 23
2.5. Classification of SYN flooding Detection Schemes ........................................... 24

IV
5.4 Comparison of Results from new DoS detection system to results from Wireshark

5.5. Summary

CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS

6. Introduction

6.1 Conclusion of the project

6.2 Significant Contribution

6.3 Limitation of the Research

6.4 Recommendations and future work

References

Appendix A

Appendix B
LIST OF TABLES

Chapter one:
Table 1.1: Examples of Threats ........................................................................................................3

Chapter Two:
Table 2.1: Advantages and weakness for router Scheme ......................................................... 27
Table 2.2: Advantages and weakness for statistical analysis .................................................... 29
Table 2.3: Advantages and weakness for fuzzy logic and neural network ..............................32

Chapter Three:
Table 3.1: Hardware Requirements .......................................................................................... 43
Table 3.2: Software Requirements ........................................................................................... 44

Chapter Four:
Table 4.1: Functional requirement .......................................................................................... 51
Table 4.2: Non-functional requirement .................................................................................... 54
Table 4.3: Use Case Login (UC_01) ........................................................................................ 57
Table 4.4: Use Case start/ stop (UC_02) .................................................................................. 58
Table 4.5: Use case add authenticated IP/ MAC address (UC_03) ...................................... 60
Table 4.6: Use Case remove IP/ MAC address (UC_04) .......................................................... 61
Table 4.7: Use case list all authenticated IP/ MAC address (UC_05) ...................................... 62
Table 4.8: Use case check captured packet (UC_06) ............................................................... 64

Chapter Five:
Table 5.1: Overall detection percentage .................................................................................. 89
LIST OF FIGURES

Chapter One:
Figure 1.1: Research Landscape Pyramid..............................................5
Figure 1.2: A Local Area Network (LAN).................................................6
Figure 1.3: SYN-Flooding attack scenario .............................................10
Figure 1.4: Ping flood attack.................................................................11
Figure 1.5: Ping of Death (POD) Attack................................................11
Figure 1.6: Distributed Denial of Service (DDoS) Attack........................12

Chapter Two:
Figure 2.1: IPv4 header structure..........................................................22
Figure 2.2: Denial of Service Attacks (DoS) classification schemes ..........25
Figure 2.3: Router based Counter Bloom Filter (CBF) Scheme...............26
Figure 2.4: The proposed system based on fuzzy logic .........................32

Chapter Three:
Figure 3.1: General Methodology for Design Research (GMDR)...........38
Figure 3.2: The overall framework of a new DoS detection system .........41
Figure 3.3: Extreme programming .......................................................43

Chapter Four:
Figure 4.1: New DoS detection framework in details............................55
Figure 4.2: Use case diagram for new DoS system ................................56
Figure 4.3: Login sequence diagram...................................................66
Figure 4.4: Register sequence diagram..............................................67
Figure 4.5: New DoS detection system.................................................68
Figure 4.6: Login collaboration diagram.............................................70
Figure 4.7: Register collaboration diagram.........................................70
Figure 4.8: collaboration diagram for new DoS Detection System........71
Figure 4.9: Class Diagram for new Dos detection system......................72
Figure 4.10: New Dos detection system main page...............................73
Figure 4.11: Registration page for new DoS detection system.................73
Figure 4.12: Login page for new DoS detection system.........................74
Figure 4.13: Managing IP/ MAC address in new DoS detection system ....75
Figure 4.14: Add/ Update/ Delete/ View MAC address in new DoS detection System .................................................................75
Figure 4.15: Add/ Update/ Delete/ View IP address in new DoS detection System ..76
Figure 4.16: Add IP address Page.......................................................76
Figure 4.17: Add MAC address Page...................................................77
Figure 4.18: New DoS detection system page......................................78
Figure 4.19: Authenticated IP is captured in the new DoS detection system ....79
Figure 4.20: Detection SYN flooding attack in a real time ...................80
Figure 4.21: Display all packet Information........................................81
Chapter Five:
Figure 5. 1: Pseudo code SYN flooding Detection ............................................. 84
Figure 5. 2: SYN flooding attack scenario .......................................................... 85
Figure 5. 3: Two SYN flooding attacks scenario ................................................. 86
Figure 5. 4: Low-Rate SYN flooding attack scenario ......................................... 87
Figure 5. 5: Two SYN flooding and SYN flooding low agent attacks scenario .... 88
Figure 5. 6: Accuracy detection for new DoS system ......................................... 90
LIST OF APPENDIXES

Appendix A ...................................................................................................................... 99
Appendix B ...................................................................................................................... 100
# LIST OF ABBREVIATION

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management System</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>PoD</td>
<td>Ping of Death</td>
</tr>
<tr>
<td>CBF</td>
<td>Counting Bloom Filter</td>
</tr>
<tr>
<td>TTL</td>
<td>Time to Live</td>
</tr>
<tr>
<td>TP</td>
<td>True Positive</td>
</tr>
<tr>
<td>TN</td>
<td>True Negative</td>
</tr>
<tr>
<td>FP</td>
<td>False Positive</td>
</tr>
<tr>
<td>FN</td>
<td>False Negative</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modelling Language</td>
</tr>
<tr>
<td>XP</td>
<td>Extreme Programming</td>
</tr>
<tr>
<td>JPcap</td>
<td>Java Packet Capture</td>
</tr>
</tbody>
</table>
CHAPTER ONE

INTRODUCTION

This chapter briefly provides the research landscape and elaborates the main concepts leading to the conception of a novel detection system for Denial of Service attacks.

Section 1.1 describes the top-bottom research landscape and hierarchical architecture while providing important concepts pertaining to the network architecture and service related to the research undertaken. This is crucial in laying the foundation for understanding the intricacies of the research undertaken and paves the way for elucidating the impetus of the research work involved. This leads to Section 1.2 on the motivation of the research, followed by the problem statement, in Section 1.3, the corresponding research questions in Section 1.4, the objectives of the study in Section 1.5, the scope of the study in Section 1.6 and the significance of the study in Section 1.7. Finally, Section 1.8 provides the organization of the remaining chapters of the report.

1. Introduction

Information has become an organization’s most precious asset. Organizations have become increasingly dependent on information. The widespread use of e-commerce has increased the necessity of protecting the system to a very high extent (Botha, Von Solms, Perry, Loubser, & Yamoyany, 2002), (P. Kiran Sree, 2008).

Within an organization, information is typically located on servers that are shared by the entire organization or by individual units. Alternatively, information
The contents of the thesis is for internal user only
References


Conference on Wireless Communications, Networking and Mobile Computing, USA: IEEE.


