ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

ARCHITECTURE AND CLASSIFICATION OF DDOS ATTACKS

M.PadmavathyM.Sc (CS)., M.Phil.,
Research Scholar, Department of Computer Applications,
School of Information Technology, Madurai Kamaraj University,
Palkalainagar, Madurai – 625021.
E-Mail: padmaphd1@gmail.com

Dr. M. Ramakrishnan, M.E., Ph.D., Ph.D.
Professor and Head Department of Computer Application
Chairperson - School of Information Technology Madurai Kamaraj University
Madurai – 625 021.

Abstract— **Distributed Denial of Service (DDoS) Attacks has been increasingly found to be affecting the normal functioning of organizations causing billions of dollars of losses. Organizations are trying their best to minimize their losses from these systems. This paper presents a structural approach to the DDoS problem by developing a classification of DDoS attacks and DDoS defense mechanisms.[1] Furthermore, important features of each attack and defense system category are described and advantages and disadvantages of each proposed scheme are outlined.We survey different papers describing methods of defense against DDoS attacks based on entropy variations, traffic anomaly parameters, neural networks, device level defense, botnet flux identifications and application layer DDoS defense.**

Keywords: DDoS, Intrusion Prevention System, Classification of DDoS Attacks, Classification of DDoS Defense Systems.

Introduction

I. Introduction to DDoS

Overview of DoS

Denial of service attack

Denial of service attack is an attempt by an attacker to exhaust the target's computational and network resources so that legitimate users cannot gain access the target's services. [2]

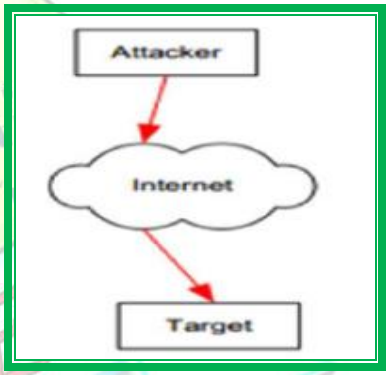

Fig 1. DOS Attack

- Background Information: Denial of Service Attacks.
- Classification of Denial of Service Attacks.
- Countermeasures for Denial of Service Attacks.
- Denial of Service Attacks Shortfalls.

Overview of DDoS

Distributed denial of service attack

DDOS attack is an attempt by an attacker when many compromised and vulnerable systems are infected by the malicious code simultaneously and these compromised machines are coordinated under the control of a single attacker in order to break the victim's system and exhaust its resources. [2]

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

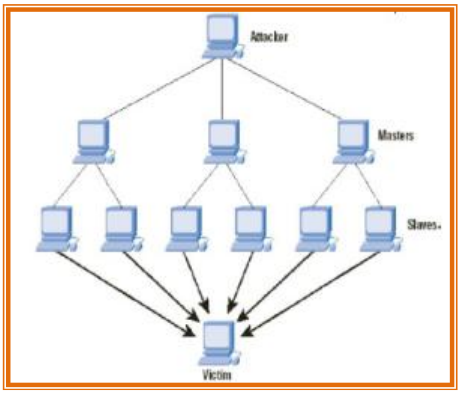

Fig 2. DDOS Attack

- Distributed Denial of Service Attacks.
- Distributed Denial of Service Attack Architecture.
- Widely Used Distributed Denial of Service Tools.
  - ✓ Trinoo
  - ✓ TFN/TFN2K
  - ✓ Stacheldraht
- Common DDoS Countermeasures.
- DDoS Protection Environment.

II. DDOS ATTACK CLASSIFICATION

There are two types of attacks in terms of the number of malicious entities.

- Uni-Source attacks- These attacks are sent from a single machine or launched by a single source.
- Distributed attacks- These attacks are sent from a multiple machines or originating from multiple sources. [4]

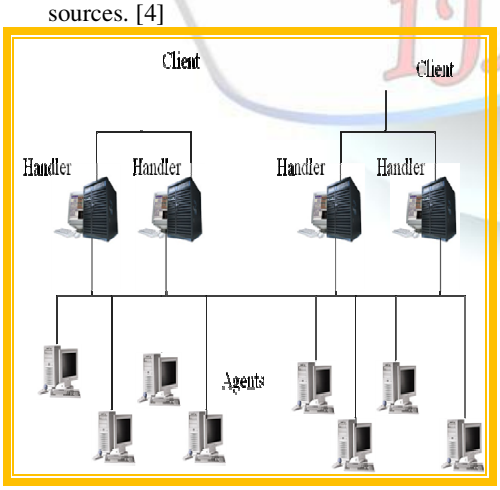

Fig 3. DDoS Architecture

There are two types of DDOS attacks, Bandwidth depletion attack and Resource depletion attack.

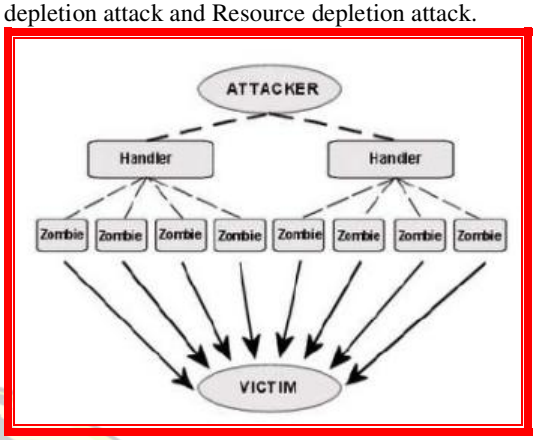

Fig 4. Architecture of DDoS Attack

IV. TYPES OF DDoS ATTACKS

Two types of DDoS attacks

- ✓ Flooding,
- ✓ Scanning attacks.
- ✓

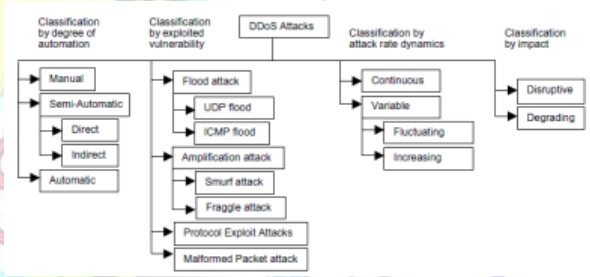

Fig 5. Classification of DDoS attacks.

V. CONCULSION

DDOS attacks are one of the most dangerous threats to the computer networks.Distributed denial of service attacks is a complex and serious problem and consequently, numerous approaches have been proposed to counter them. The multitude of current attack and defense mechanisms obscures the global view of the DDoS problem. It is important to recognize and understand trends in attack technology in order to effectively and appropriately evolve defense and response strategies.The most serious attack for network security is DDoS (Distributed Denial of Service) attack.The more the rate of the internet usage increases, the more challenge increase for efficient DDos detection system.So there are many challenges for detecting and classifying DDoS attacks.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

VI. REFERENCES

1) Distributed Denial of Service Attacks,Ali Bayazit,Qiang Huang,Stephan Specht,September 23, 2002,Princeton University Electrical Engineering Department.
2) A Statistical Approach to Classify and Identify DDoS Attacks using UCLA Dataset Thwe Thwe Oo, Thandar Phyu,ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, May 2013.
3) Detection Architecture of Application Layer DDoS Attack for Internet Sanjay B Ankali,Dr. D V Ashoka,Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:984-990 (2011).
4) Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System Mohd. Jameel Hashmi1, Manish Saxena2 and Dr. Rajesh Saini3,Manish Saxena et al , International Journal of Computer Science & Communication Networks,Vol 2(5), 607-614 ISSN:2249-5789.
5) DDoS Attack and Defense: Review of Some Traditional and Current Techniques,Muhammad Aamir and Mustafa Ali Zaidi SZABIST, Karachi, Pakistan.https://www.jstage.jst.go.jp/article/iis/19/2/19_IIS190208/_article DOI: 10.4036/iis.2013.173.
6) DDoS attacks and defense mechanisms: classification and state-of-the-art Christos Douligeris *, Aikaterini Mitrokotsa Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece Received 9 October 2003; accepted 13 October 2003 Responsible Editor: I.F. Akyildiz,www.elsevier.com/locate/comnet.
7) AN OVERVIEW OF CLASSIFICATION OF DDOS ATTACKS AND DEFENCE MECHANISMS FOR DDOS ATTACKS Rasleen Kaur, Randeep Kaur,Kaur, et al., International Journal of Advanced Engineering Technology E-ISSN 0976-394.Department of Computer Engineering, Global Institute of Management & Technology, Amritsar, Punjab, India.
8) Classification of Distributed Denial of Service Attacks – Architecture, Taxonomy and ToolsILovepreet Kaur Somal, IIKaranpreet Singh VirkI,IIM.Tech Student, Dept. of Computer Engineering, Punjabi University Patiala, Punjab, India. International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) © 2014, IJARCST All Rights Reserved 118 Vol. 2, Issue 2, Ver. 1 (April - June 2014)ISSN : 2347 - 8446 (Online) ISSN : 2347 - 9817 (Print).