Detection and analysis of DoS Attack

Amrasha M Hegde
Department of ISE
NMAMIT, Nitte
Karnataka
4nm18is011@nmamit.in

Anjan S Madhyastha
Department of ISE
NMAMIT, Nitte
Karnataka
4nm18is015@nmamit.in

Shraddha JR
Department of ISE
NMAMIT, Nitte
Karnataka
4nm18is0107@nmamit.in

Shreya Kamath S
Department of ISE
NMAMIT, Nitte
Karnataka
4nm18is110@nmamit.in

Abstract*— *Nowadays, e-community business, web servers and organizations, mainly suffered by Denial of Service (DoS) attacks. DoS is a common attack causes significant problems in business operations and 65% organizations are suffering over the Internet. This type of attack is created by sending a high rate malicious traffic towards the server and block genuine users using desired network sources and services. In this way this attack consumes the network resources and services which results into degrades the availability of desired services to the valid users. A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attack typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateway and even root name servers. There are two general forms of DoS attacks: those that crash services and those that flood services. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attack are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing media between the intended users and the victim.

Keywords—Wireshark, Ping attack, Syn flood attack

I. INTRODUCTION

DOS attack is an attack on the computer or network that restricts, reduces, or prevents the system from restoring accessibility to its legitimate users. It is a kind of attack in which an attacker or intruder tries to deprive system users or authorized users of accessing their computers, networks, or sites. Here the attacker focuses on the bandwidth of the victim to perform this attack.

Malicious use of resources internally within an organization may also result in a Denial of Service attack. The target computers can also be attacked from the internal network by an unsatisfied or disgruntled employee. It can also be executed against network resources, data access within an inter-networked environment. In 95% of cases, an attacker's motive using this Denial of Service is destruction and not stealing.

In this project we used two different types of attacks they are:-

SYN Flood attack **:** A SYN flood is a form of denial-of-service attack in which an attacker rapidly initiates a connection to a server without finalizing the connection. The server has to spend resources waiting for half-opened connections, which can consume enough resources to make the system unresponsive to legitimate traffic.

Ping Flood Attack:- A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP "echo request" (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. Most implementations of ping require the user to be privileged in order to specify the flood option. It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem). The attacker hopes that the victim will respond with ICMP "echo reply" packets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.

II. RELATED WORKS AND REFERENCES

Denial of service (DoS) attacks have become a major threat to current computer networks. To have a better understanding on DoS attacks, this article provides an overview on existing DoS attacks and major defense technologies in the Internet and wireless networks. In particular, we describe network based and host based DoS attack techniques to illustrate attack principles. DoS attacks are classified according to their major attack characteristics. Current counterattack technologies are also reviewed, including major defense products in deployment and representative defense approaches in research. Finally, DoS attacks and defenses in 802.11 based wireless networks are explored at physical, MAC and network layers.[1]

Denial of Service (DoS) and distributed denial of service attack (DDoS) is now a common means of attack that affects seriously network security and the quality of online services. This paper analyzes the DoS (DDoS) attack prevention principles and gives an thorough analysis of existing prevention techniques, proposed to prevent DoS (DDoS) attacks in three ways: using a router DoS attack prevention, increase the trusted platform module, increase system defenses.[2]

They describe a specification-based approach to detect exploitations of vulnerabilities in security-critical programs. The approach utilizes security specifications that describe the intended behavior of programs and scans audit trails for operations that are in violation of the specifications. We developed a formal framework for specifying the security-relevant behavior of programs, on which we based the design and implementation of a real-time intrusion detection system for a distributed system. Also, we wrote security specifications for 15 Unix setuid root programs. Our system detects attacks caused by monitored programs, including security violations caused by improper synchronization in distributed programs. Our approach encompasses attacks that exploit previously unknown vulnerabilities in security-critical programs.[3]

III. METHODOLOGY

1.Algorithm for detection of SYN Flood Attack:-

At first capture the packets in Wireshark before the syn flood attack and save the pcap file as P1.Then send attack using hping3 in command prompt in kali linux to the respective target. Command used here is:

Hping3 -S -p <port number> - - flood - -rand-source <Destination IP address>

Here either we can spoof the Ip address using-a or can use rand-source to generate some random Ip address. Capture the packets in Wireshark after the syn flood attack and save the pcap file as P2. Check the number of syn packets and syn ack packets after the attack. . Send the both pcap files as input to the python code.. From the output of the python code a two graphs are obtained where the number of TCP will be more in P2 compared to P1 this confirms that there is an syn flood attack thus dos attack using syn flood attack is detected and analysed.

2.Algorithm for detection of PING Flood Attack(ICMP Flood Attack):-

Capture the packets in Wireshark before the icmp flood attack and save the pcap file as P1. Send attack using hping3 in command prompt in kali Linux to the respective target. Command used here is:

Hping3 -1 -p <port number> - - flood - -rand-source <Destination IP address>

Here either we can spoof the Ip address using -a or can use rand-source to generate some random Ip address. Capture the packets in Wireshark after the icmp flood attack and save the pcap file as P2.Check number of echo requests after the attack. Send the both pcap files as input to the pythoncode. From the output of the python code a two graphs are obtained where the number of ICMP will be more in P2 compared to P1 this confirms that there is an icmp flood attack thus dos attack using icmp flood attack is detected analysed.

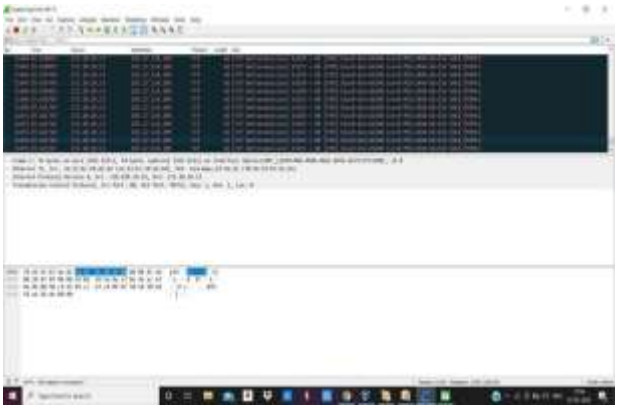
a)Python Code used for analysis of number of packets:-

In this python code we imported packages like pyshark, matplotlib, collections and numpy. Here pcap files are given as input and then graph is obtained showing the number of packets used for analysis.

IV. RESULT AND DISCUSSION

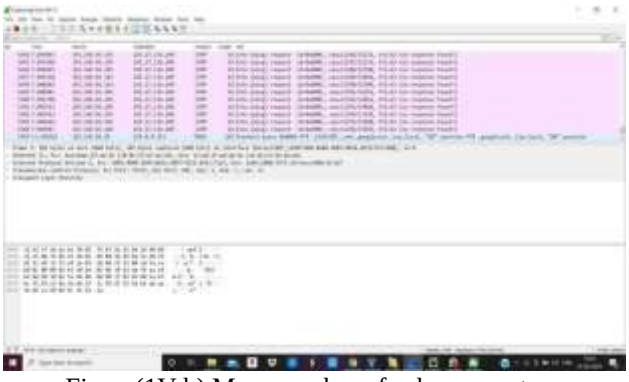
A DoS or Denial-of-Service attack is an attack targeting the availability of web applications. Unlike other kinds of attacks, the primary goal of a DoS attack is not to steal information but to slow or take down a web site. It shows how many web applications have been effected from this attack with the help of tools like wireshark which makes the process easy to capture and verify any suspicious of a DoS attack and we have used python code to analyze those number of packets.

a) Capturing syn packets in Wireshark:-



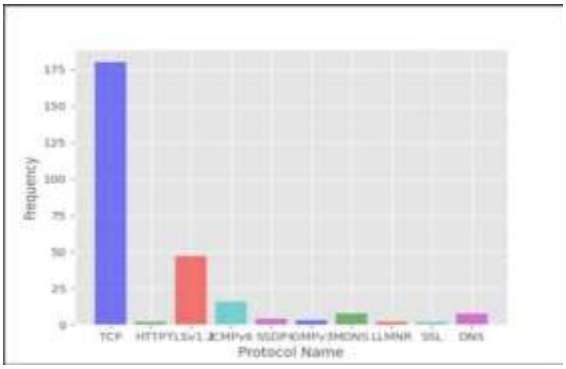
Figure(1V.a) More number of syn packets

b)Capturing icmp packets in Wireshark:-



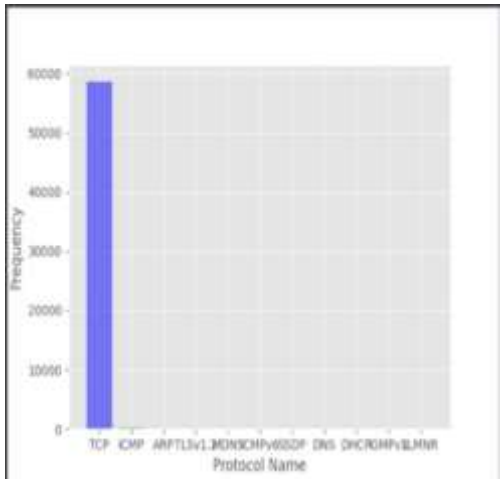
Figure(1V.b) More number of echo requests

c) Before SYN FLOOD/PING FLOOD Attack:-



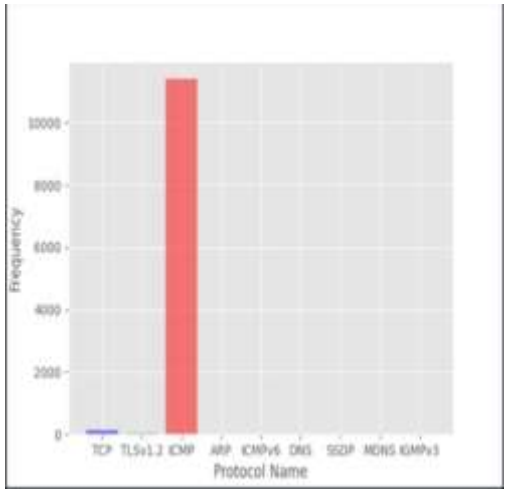
Figure(1V.c) Graph before syn/ping flood attack

d)After SYN FLOOD Attack:-



Figure(1V.d) Graph obtained after syn flood attack

e) AFTER PING FLOOD ATTACK:-



Figure(1V.e) Graph obtained after ping flood attack

From these results we can analyze that number of TCP is increased after the syn flood attack and number of ICMP increased after icmp flood attack thus we detected and analyzed these two attacks.

V.CONCLUSION

As described Dos attack is an attack targeting the availability of web applications& unlike other kinds of attacks, the primary goal of a DoS attack is not to steal information but to slow or take down a web site. Here, the attackers (hackers) attempt to prevent legitimate users from accessing the service.So in this project we have detected and analyzed two types of dos attacks that is syn flood attack and ping flood attack which can cause damage to the website.In order to successfully defend against present types of denial of service attacks and gain insight to future possibilities, it is crucial to develop a clear image of the broad spectrum of existing attacks and countermeasures. Although no “silver bullet” solution to the problem of denial of service attacks currently exists, various countermeasures can make attacks far more difficult to successfully devise and execute.

Counter measure for DOS attacks are:-

- Use up-to-date anti-virus and IDS tools.
- Perform network analysis to find out the possibility of DOS attack.
- Shut down unnecessary services in the target network.
- Find and neutralize handlers. Protect secondary victims.
- Perform proper activity profiling and ingress/egress filtering to filter out unwanted traffic.
- Enforce in-depth packet Analysis.
- Use Defense-in–depth approach.
- Add additional load balancers to absorb traffic and set up throttle logic to control traffic.

VI. ACKNOWLEDGEMENT

It is with great satisfaction and euphoria that we are submitting the Mini Project Report on “DETECTION AND ANALYSIS OF DOS(Denial of Service)ATTACK”. We have completed it as a part of the curriculum of Visvesvaraya Technological University, Belagavi for the award of Bachelor of Engineering in Information Science and Engineering.We are profoundly indebted to our guide Mr. Vasudeva Pai, Mini Project Coordinators & Assistant Professor, Department of Information Science & Engineering for their constant encouragement and support extended throughout.We express our sincere gratitude to Dr. Karthik Pai B H, Head and Associate Professor, Department of Information Science and Engineering for his invaluable support and guidance.We sincerely thank Dr. Niranjan N Chiplunkar, Principal, NMAM Institute of Technology, Nitte and Dr. I Ramesh Mithanthaya, Vice Principal & Dean (Academics), NMAM Institute of Technology, Nitte, who have always been a great source of inspiration.Finally, yet importantly, we express our heartfelt thanks to our family and friends for their wishes and encouragement throughout the work.

VII. REFERENCES.

[1] Denial of Service Attacks Qijun Gu, PhD. Assistant Professor Department of Computer Science Texas State University – San Marcos San Marcos, TX, 78666.

[2] DOS Attack Analysis and Study of New Measures to Prevent.

[3] Execution monitoring of security-critical programs in distributed systems: a specification-based approach

[4] K. Ilgun, "USTAT: A real-time intrusion detection system for Unix", *Proceedings of the 1993 Symposium on Security and Privacy*, pp. 16-28, 1993-May-24-26.

[5] A survey of distributed denial-of-service attack, prevention, and mitigation techniques

[6] Waterman, S. DDoS attacks growing faster in size, complexity—arbor report, 2017, (accessed 10 March 2017).

[7] Deng, J, Han, R, Mishra, S. Limiting DoS attacks during multihop data delivery in wireless sensor networks. Int J Secur Network 2006; 1(3–4): 167–178.