Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention of DoS Attack

Bahubali Akiwate, Manasi Desai, Shweta Surpurmath
Rohit khot, Deepak Power, Dept of CSE, K.L.E College of Engineering and Technology, Chikodi, Karnataka, India

Abstract- Amongst various online attacks hampering IT security, Denial of Service (DoS) has the most devastating effects. It has also put tremendous pressure over the security experts lately, in bringing out effective defense solutions. These attacks could be implemented diversely with a variety of tools and codes. Since there is not a single solution for DoS, this attack has managed to prevail on internet for nearly a decade. Hence, it becomes indispensable to carry out these attacks in small test bed environments in order to understand them better. Unlike other theoretical studies, this project lays down the steps involved in implementing these attacks in real time networks. These real time attacks are measured and analyzed using network traffic monitors. In addition to that, this approach also details various defense strategies that could be enabled on Cisco routers in order to mitigate these attacks. Some of the most exciting attacks done on networks today are those that are difficult to track, and requires very minimal effort on the attacker's part. Denial of Service (DoS) has the most destructive effects among the various online attacks which is hindering the security. The security experts are in tremendous pressure, to bring out effective defence solutions for the various attacks occurring recently. Variety of tools and coding are used to implement these destructive attacks. DoS attack has managed to exist in the internet for more than a decade as there is no steady solution to prevent this attack. The Intrusion prevention system is used as an extension of Intrusion detection system as a prevention technique for the DoS attacks. Network Intrusion Detection and Prevention system analyzes the packets coming and going through the interface. The paper provides the idea of various types of DoS attacks, detecting them and preventing them. There are many methods which are available to detect and resist the DoS attack. The detection and prevention techniques shown are effective for small network topologies and can also be extended to analogous large domains.

Keywords- Denial of Service (DoS), Distributed Denial of Service, System security.

I. INTRODUCTION

Denials of service (DoS) attacks pose an immense threat largely to the Internet and also the network systems and many defence mechanisms have been proposed to overcome the problems. Attackers try constantly to modify their attack methods to surpass the security systems and researchers in turn modify their approaches to handle such attacks. The DoS attack is becoming more and more complex now a day. There is variety of known attacks which creates the impression that the problem space is more, and hard to explore. The existing systems employ various techniques to counter the problem, and it is difficult to understand their similarities and differences and to evaluate their effectiveness and cost.

Denial of Service is an attack which makes an information or data unavailable to its intended hosts. This attack can be carried out in various ways and various strategies are mentioned. The underlying aspect would be to congest victim's network and thus make it inaccessible by other client. There are many other ways of making service unavailable rather than just flooding it with abundant IP packets. The victim could also be attacked at various loopholes making it unstable which depends on the nature of the attack. There are many manifestations of Denial of Service attacks but they ultimately have the same objective that is to deny or degrade users' ability to legitimately access network. DoS attacks are accomplished by draining the limited resources of network bandwidth by flooding with packets or exhausting host resources by consumption of CPU cycles, random memory, static memory or data structures .DoS attacks can generally be classified as either a Flood Attack or a Malformed Packet Attack and that where attacks originate simultaneously from several compromised sources that these can be classified as Distributed DoS attacks.

II. OBJECTIVES

- It provides the network user which is unable to access resources like e-mail and the Internet. An attack can be directed at an operating system or at the network.
- Internet to break into computers and using them to attack a network. Hundreds or thousands of computer systems across the Internet can be turned into "zombies" and used to attack another system or website.
- It provides a clear and thorough coverage of the area of DoS attacks and DoS defense approach is to improve the security level of a computer system or network.
- It is reduced by disabling unused services if there are less application services and open ports in hosts, there will be less chance of exploiting the vulnerabilities by attackers.
- When a denial of service (DoS) attack occurs, a computer or a network user is unable to access resources like e-mail and the Internet; hence is an attempt to prevent the legitimate users from accessing he network resource such as website, computer system or web service etc.

III. METHODOLOGY

A. Modules

1. Server Module
2. Local-Machine Module
3. Client Module

- **Server Module**
  In this module receive the requests and processes it made by the user. It is provided with the Eclipse tool and maintains the database and manages a queue for requests.
- **Local Machine Module**
  In this module the Local Machine sends the continuous requests to the server. Server and Client reside on Local machine itself here.
- **Client Module**
  In this module the client tries to retrieve the information from the server by sending many requests at a time through login window.

B. Implementation

Enable the connection between two systems using LAN cable taking one as Client side and another one as Server side. Confirming the connection using PING command. Check for the proper file sharing. Set the maximum number of requests to 10 and blocking time for 10 minutes at server side. At the beginning open the ORACLE Data Base and run the query to check data is present or not ; Now user tries to login and sends request to the server using User Name and Password, by clicking on LOGIN button which hits the requests to the server. Check the Data Base to ensure Number of hits, IP Address, Timing and Status (BLOCKED OR UNBLOCKED). If the Number of hits is greater than the set value the user is blocked automatically by providing the error message.

IV. OBSERVATIONS

- This figure 1 represents the log-in to the oracle database. It stores the login information of user, present at the server side.

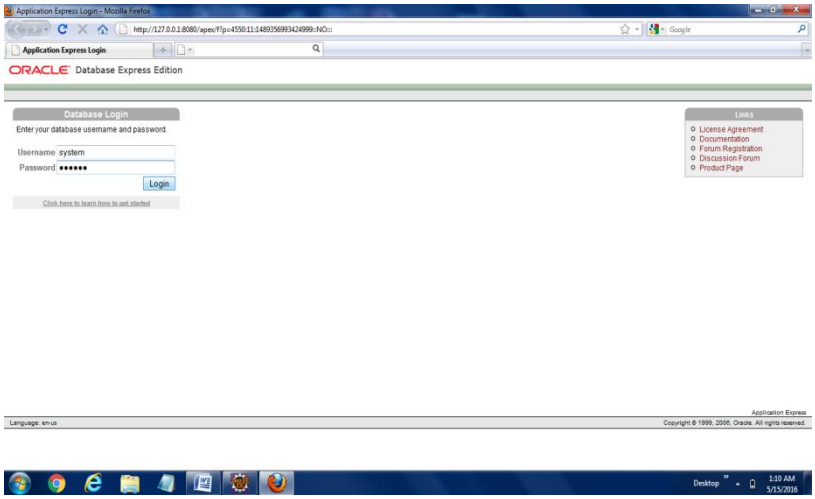

Figure 1. User login

- The figure 2 shows the Connection to the database. It connects the database with the server. Provides the successful message after connection.

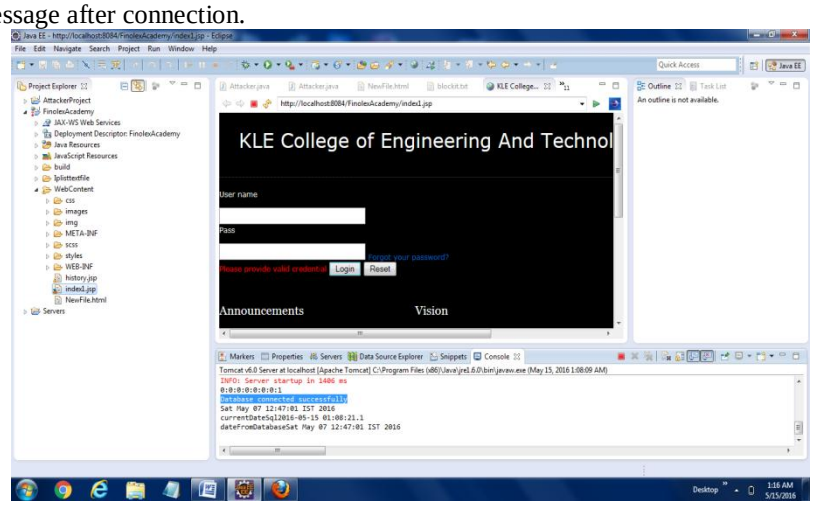

Figure 2: Database connection

- The figure 3 represents the login window at the client side through this window the user can login.

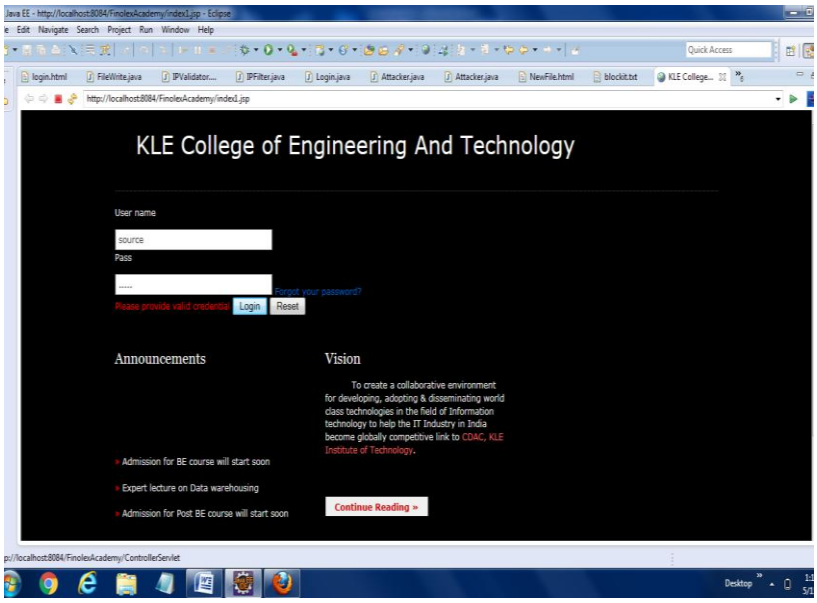

Figure 3: Client side login window

- Requests More Than That of Set Value: If user tries to attempt more than the set value of requests, the blocking message will be generated providing status as "BLOCKED".

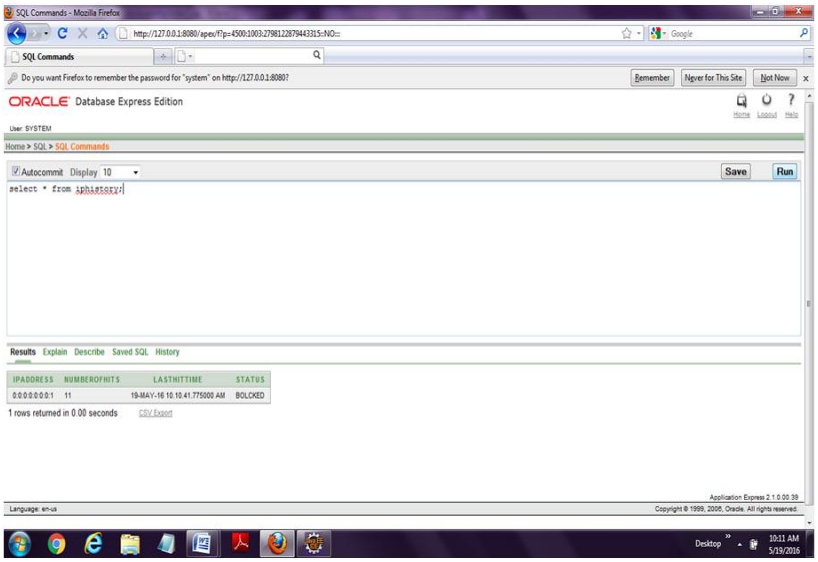

Figure 4: Blocked status of a user

IV. CONCLUSION

Denial of service attacks are a real threat to the operation of any networked computer system. While they can be difficult to detect and react to, prudent planning and preparation can mean the difference between a total shut down of the organization and a slight inconvenience. The DoS management framework presented provides coverage of security before an incident, during an incident and after an incident. While developing a DoS defence scheme, the issues discussed are needed to be deliberated and considered with due seriousness.

This approach gives the reader adequate knowledge on how to detect and prevent Denial of Service attacks. It highlights various attack tools and the ways to identify the same in a given network. It also suggests basic mitigation strategies that could be adopted in order to defend attacks. However, serious challenges arise when IPv6 needs to be established globally and transition from version 4 to version 6 has to be done. IPv6 introduces six optional headers like Routing header, Authentication header etc. In spite of providing better security with authentication, encryption and encapsulation techniques, IPv6 also brings out serious complications. The following two types of Denial of Service attacks could be implemented if IPv6 is used.

REFERENCES

[1] Gupta, B. B., Joshi, R. C., and Misra, M. (2012) ANN based scheme to predict number of zombies in DoS attack. International Journal of Network Security, 14, 36–45.

[2] Francois, J., Aib, I., and Boutaba, R. (2012) Fire Col: A collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Transaction on Networking.

[3] Yu, S., Zhou, W., Doss, R., and Jia, W. (2011) Trace back of DDoS attacks using entropy variations. IEEE Transaction on Parallel Distributed Systems, 22, 412–425.

[4] Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions Monowar H. Bhuyan1, H. J. Kashyap1, D. K. Bhattacharyya1 and J. K. Kalita2 Tezpur-784028, Assam, India 2Department of Computer Science, University of Colorado at Colorado Springs, CO 80933-7150, USA.

[5] Subramani Rao, Sridhar Rao, "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis", SANS institute Infosec Reading Room Sep 11, 2011.

[6] Suchitha Patil, Dr.B.B. Meshram, "Network Intrusion Detection and Prevention Techniques", International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012

