*International Journal of Latest Engineering and Management Research (IJLEMR)*
*ISSN: 2455-4847*
*www.ijlemr.com || Volume 02 - Issue 07 || July 2017 || PP. 35-40*

# Recent Study of Denial of Service Attack Types and Preventions

Jitendra Jain[1], Dr. Parshuram Pal[2]
*[1](Research Scholar, Faculty of Computer Science), Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan, India*
*[2](Professor, MCA , Lakshmi Narain College of Technology,Bhopal, M.P., India*

**Abstract:** A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent valid users from accessing the service. Attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy. In this paper we proposed a study of DoS attacks, types of DoS attacks, several ways that ac be used for a DoS attack and prevention from DoS attack.

**Keywords:** Dos Attack,

## I. Introduction

The first detection of DoS attack was found in 1988 in Carnegie Mellon US. A more alarming attack occurred identified to be due to Denial of Service Attack. In February 2000 Yahoo portal was shut down for 3 hours due to DoS, in that evening, eBay (EBAY), Amazon.com (AMZN), and CNN (TWX) had gone down.

A DoS attack can be done in a several ways. The basic types of DoS attack include:

1. Flooding the network to prevent legitimate network traffic
2. Disrupting the connections between two machines, thus preventing access to a service
3. Preventing a particular individual from accessing a service.
4. Disrupting a service to a specific system or individual
5. Disrupting the state of information, such resetting of TCP sessions

Another variant of the DoS is the smurf attack. This involves emails with automatic responses. If someone emails hundreds of email messages with a fake return email address to hundreds of people in an organization with an auto responder on in their email, the initial sent messages can become thousands sent to the fake email address. If that fake email address actually belongs to someone, this can overwhelm that person's account.

DoS attacks can cause the following problems:

1. Ineffective services
2. Inaccessible services
3. Interruption of network traffic
4. Connection interference

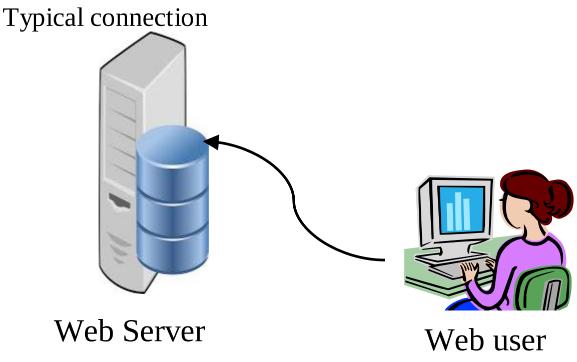

Figure 1 Try to connect server to authenticate

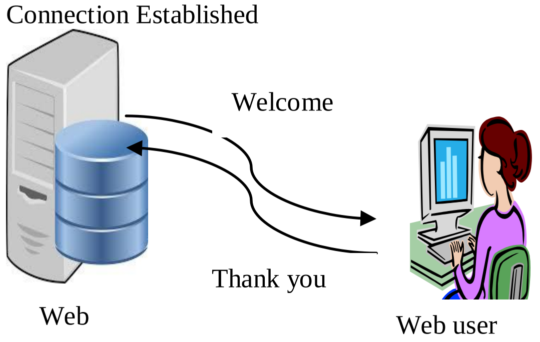

Figure 2 Server returns the authentication approval

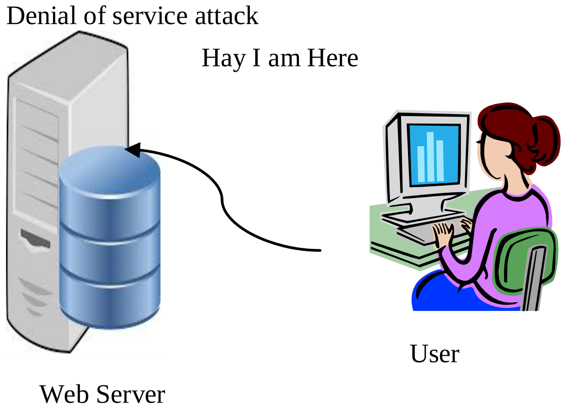

Figure 3 Try to connect server to authenticate

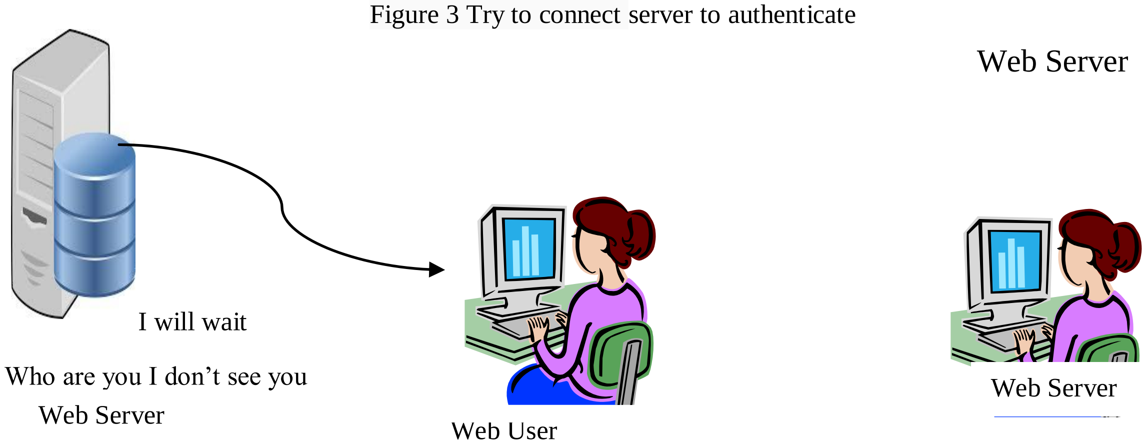

Figure 4 Effected with DoS attack

## II. How DOS Works

In a typical connection, the user sends a message asking the server to authenticate it. The server returns the authentication approval to the user. The user acknowledges this approval and then is allowed onto the server.

In a denial of service attack, the user sends several authentication requests to the server, filling it up. All requests have false return addresses, so the server can't find the user when it tries to send the authentication approval. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again--tying up the service indefinitely.

## III. Literature Survey

In 2013 Kanikaet al proposed “Security of Network Using IDS and Firewall”. They proposed a study over IDS and Firewall. They show that IDS is mainly used for detecting break-ins or misuse of the network. IDS are the ‘burglar alarm’ for the network because much like a burglar alarm, IDS detects the presence of an attack in the network and raises an alert. An IDS provides three functions monitoring, detecting and generating an alert. IDS is a system that will constantly monitor the corporate networks from all types of attacks and vulnerabilities. IDS looks for the attack signatures which are specific patterns that usually indicate malicious or suspicious event.

In 2014 Milan Jain proposed “Malicious Code Detection through Data Mining Techniques” . They explore the application of data mining methods to predict rootkits based on the attributes extracted from the information contained in the log files. The rootkit records were categorized as Inline and other based on the attribute values. They proposed three algorithms named as RIPPER, Naives Bayes approach, and Multi-Naïve Bayes using data mining techniques and the comparison of these algorithms.

In 2015 Mohsen Kakavand et al proposed “A Survey of Anomaly Detection Using Data Mining Methods for Hypertext Transfer Protocol Web Services”. They provided an overview on four general data mining techniques such as classification, clustering, semi-supervised and association rule mining. These data mining anomaly detection methods can be used to computing intelligent HTTP request data, which are necessary in describing user behavior. To meet the challenges of data mining techniques, provide challenges and issues section for intrusion detection systems in HTTP web services.

In 2016 Mridalini Gupta et al proposed “Intrusion Detection Using Decision Tree Based Data Mining Technique” They proposed research work introduces a framework to develop a classifier based on data mining techniques. In the

proposed framework ORNL dataset is given to Pre-processing stages which classify in j48 algorithm and reduce irreverent features from the data set so that data with less number of features will require tofeed to the classifier and will provide efficiency to the classifier. Machine learning tools WEKA are used to analyze the performance of datasets.

In 2017 Jithin Mathew et al Proposed “Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection”. Proposed survey describes a focused literature survey of machine learning and data mining methods for cyber analytics in support of intrusion detection. Based on the number of citations or the relevance of an emerging method, papers representing each method were identified, read, and summarized. Because data are so important in machine learning and data mining approaches, some well-known cyber data sets used in machine learning and data mining are described for cyber security is presented, and some recommendations on when to use a given method are provided.

## IV. Seven Common DDOS Attack Tools

Just as the network security and hacking world is continually evolving, so too are the tools used to carry out distributed denial of service (DDoS) attacks. For example, DDoS tools such as Trinoo were widely used at the turn of the century, but these tools ran only on the Linux and Solaris operating systems. Specialized DDoS attack tools have since evolved to target multiple platforms, rendering DDoS attacks more dangerous for targets and much easier for hackers to carry out.

Some of the newer DDoS tools such as Low Orbit Ion Cannon (LOIC) were originally developed as network stress testing tools but were later modified and used for malicious purposes. Others such as Slowloris were developed by “gray hat” hackers whose aim is to direct attention to a particular software weakness. By releasing such tools publicly, gray hat hackers force software developers to patch vulnerable software in order to avoid large-scale attacks. Here are seven of the most common - and most threatening - specialized DDoS attack tools.

### 5.5.1 LOIC

Low Orbit Ion Cannon (LOIC) is a simple flooding tool that can generate massive volumes of TCP, UDP, or HTTP traffic to subject a server to a heavy network load. LOIC’s original developers, Praetox Technologies, intended the tool to be used by developers who wanted to subject their own servers to heavy network traffic loads for testing purposes.

### 5.5.2 HOIC

HOIC is a simple cross-platform basic script for sending HTTP POST and GET requests wrapped in an easy-to-use GUI. Booster scripts also allow users to specify lists of target URLs and identifying information when generating attack traffic, making HOIC attacks anonymous and harder to block. HOIC continues to be used by Anonymous to launch DDoS attacks worldwide.

### 5.5.3 HPING

hping can be used to send large volumes of TCP traffic to a target while spoofing the source IP addresses, making it appear to be random or even to originate from a specific, user-defined source. This powerful, robust tool is among Anonymous' current DDoS attack tools of choice.

### 5.5.4 Slowloris

Developed by a gray hat hacker who goes by the handle "RSnake," Slowloris creates a DoS condition for a server by using a very slow HTTP request. By sending HTTP headers to the target site in tiny chunks as slowly as possible, the server is forced to continue to wait for the headers to arrive. If enough connections are opened to the server in this way, the server becomes unable to handle legitimate requests.

### 5.5.5 R U Dead Yet ?

Another slow-rate DDoS attack tool, R U Dead Yet? (R.U.D.Y.) achieves denial of service by using long-form field HTTP POST submissions rather than HTTP headers, as Slowloris does. By injecting one byte of information into an application POST field at a time, R.U.D.Y. causes application threads to await the end of never-ending posts in order to perform processing. Since R.U.D.Y.

### 5.5.6 #Refref

#RefRef, another tool in Anonymous' arsenal, is based on vulnerabilities in SQL database software that allow for injection attacks. Using an SQL injection, #RefRef forces a target server to use a special SQL function that repeatedly executes SQL expressions. Nonstop execution of a few lines of code consumes the target servers' resources, resulting in denial of service for a target server.

### 5.5.7 Botnets as a DDoS Attack Tool

Botnets are large collections of compromised computers, often referred to as "zombies," that are infected with malware that allows an attacker to control them. Botnet owners, or "herders," can control the machines in the botnet using a covert channel, such as IRC, issuing commands to perform malicious activities such as DDoS attacks, distribution of spam mail, and information theft.

## V. Preventative Measures

To prevent your system and network from becoming a victim of DoS attacks, CERT/CC offers many preventative solutions include. Implement router filters, install patches to guard against TCP SYN flooding. Disable any unused or unneeded network services. Enable quota systems on your operating system if they are available. Observe system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic. Routinely examine your physical security with respect to your current needs. Use Tripwire or a similar tool to detect changes in configuration information or other files. Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled. Invest in redundant and fault-tolerant network configurations. Establish and maintain regular backup schedules and policies, particularly for important configuration information. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT Administrator.

## VI. Worldwide DDOS Attacks Report

In 2016, Neustar has proposed a independent research study of 1,002 directors, managers, CISOs, CSOs, CTOs, and other c-suite executives to find out how distributed denial of service (DDoS) attacks are affecting them.

Table 1 Percentage of organizations effected with DDoS Attack

| Area | DDoS Attack | Percentage |
|---|---|---|
| North America | Organizations attacked | 70 |
| | Organizations attacked six or more times | 42 |
| | Malware activation after DDoS attack | 38 |
| East | Organizations attacked | 75 |

| | | |
|---|---|---|
| Middle Europe and Africa | Organizations attacked six or more times | 48 |
| | Malware activation after DDoS attack | 32 |
| Asia pacific | Organizations attacked | 77 |
| | Organizations attacked six or more times | 45 |
| | Ransom ware activation after DDoS attack | 16 |

In order to provide a true and global picture they surveyed participants across all six habitable continents and categorized their responses into three distinct regions.

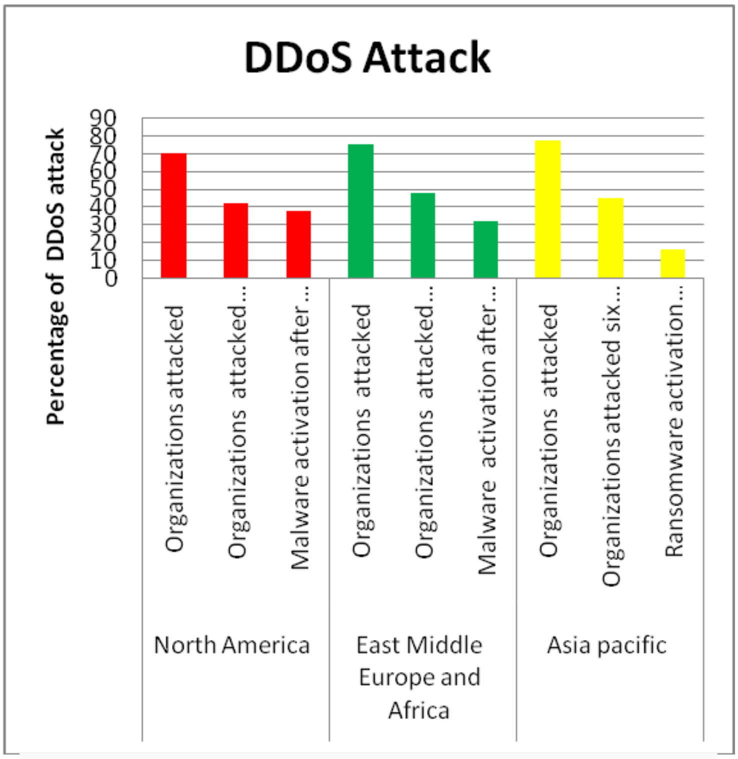

Figure 5 Percentage of DDoS attack at different area of the world

## VII. DDOS Attacks Continue In Last 12 Month

73 percentages of organizations were targeted with DDoS attack in last 12 month.

Table 2 Percentage of organizations effected with DDoS Attack

| Number of Attacks frequency | Percentage |
|---|---|
| ONCE | 11 |
| 2-5 TIMES | 29 |
| 6-10 TIMES | 14 |
| ABOUT EVERY MONTH | 10 |
| ABOUT EVERY WEEK | 5 |

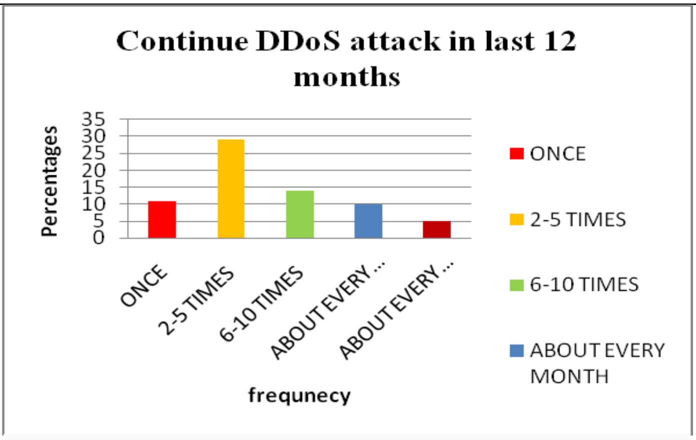

Figure 6 Percentage of DDoS Attacks Continue in last 12 month

## VIII. Conclusion

A denial-of-service (DoS) is type of attack where the attackers (hackers) attempt to prevent valid users from accessing the service. Attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. We proposed a study of DoS attacks, types of DoS attacks, several ways that ac be used for a DoS attack and prevention from DoS attack. In last year DoS attack affected Different area of the world. DoS attack effect Bandwidth and loss of bandwidth by DDos attack. Big financial loss of various companies suffers from DDoS attacks. DDoS Attacks are continually active last 12 months and future also.

## References

[1]. Kanika, Urmila et al " Security of Network Using Ids and Firewall" International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013 1 ISSN 2250-3153.

[2]. Milan Jain and Punam Bajaj " Malicious Code Detection through Data Mining Techniques" International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 5 No. 05 May 2014 554.

[3]. Mohsen Kakavand et al "A Survey of Anomaly Detection Using Data Mining Methods for Hypertext Transfer Protocol Web Services". Journal of Computer Science 2015 The Mohsen Kakavand, Norwati Mustapha, Aida Mustapha, Mohd Taufik Abdullah and Hamed Riahi. This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license.

[4]. Mridalini Gupta et al. "Intrusion Detection Using Decision Tree Based Data Mining Technique" Volume 4 Issue VII, July 2016 IC Value: 13.98 ISSN: 2321-9653 International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[5]. Jithin Mathew and S. Ajikumar " Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection" International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307.

[6]. Rajkumar et al "A Survey on Latest DoS Attacks: Classification and Defense Mechanisms" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013.

[7]. Munivara Prasad et al "DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey" Global Journal of Computer Science and Technology: E Network, Web & Security Volume 14 Issue 7 Version 1.0 Year 2014 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[8]. Darshan Lal Meena1 " Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches" Volume 2, Issue 4, April 2014 International Journal of Advance Research in Computer Science and Management Studies Research Article / Paper / Case Study Available online at: www.ijarcsms.com.

[9]. Divya Bhavasar "International Journal Of Engineering Sciences & Research Technology" ISSN: 2277-9655Scientific Journal Impact Factor: 3.449 (ISRA), Impact Factor: 2.114.

[10]. Mustafa Aijaz " Analysis of Dos and DDos Attacks" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-5, Issue-5)