A STUDY OF DENIAL OF SERVICE ATTACK WITH ITS TOOLS AND POSSIBLE MITIGATION TECHNIQUES

A. A Adeyemo[1*], K. A. Ganiyu[2]

[1*]Department of Computer Science and Information Technology, College of Computing and Communication Studies, Bowen University, Iwo, Nigeria

[2]Department of Computer Science, School of Science, The Oke-Ogun Polytechnic, Saki, Nigeria

e-mail: akinyoye2001@yahoo.co.uk, niyiganiyu@gmail.com

Corresponding Author: akinyoye2001@yahoo.co.uk, Tel: +234(0)8054774068

Abstract

The denial of service (DOS) attack is one of the most powerful and predominant attacks used by hackers to destroy the reputation of a company or an organization. The DOS attack is one of the most dangerous cyber attacks. It causes the crash of servers and disrupts service which can lead to loss of millions, depending on the extent or duration of the attack. In the past few years, hackers have employed the DOS attack to halt the service of a server due to the availability of free DOS attack tools. These tools can be blocked effortlessly by having a strong firewall. But a prevalent and smart DOS attack can evade most of the restrictions. In this paper, we will discuss the DOS attack, its variations, and the tools (Slowloris, LOIC, XOIC, HULK, and Tor's Hammer) that are used to carry out the attack. We will also examine how to thwart this attack and how not to be the part of this attack.

Keyword: *Denial of Service, cyber attack, server, hacker, firewall Slowloris, low orbit ion cannon* **(***LOIC), XOIC, HTTP Unbearable Load King (HULK), Tor's Hammer, Rate Limiting, Intrusion Detection systems (IDS) and Intrusion Prevention Systems (IPS), Access Control Lists, DDoS Simulator (DDOSIM).*

I. INTRODUCTION

A DOS attack is an effort to make a system or server unavailable for legitimate users and, finally, to take the service down. This is accomplished by loading the server's request queue with fake requests. Henceforth, the server will not be able to process the requests of legitimate users.

Generally, there are two forms of the DOS attack. The first form is the one that can crash a server. The second form of DOS attack only floods a service to bring it to halt [1].

A. DDOS or Distributed Denial of Service Attack

This is the complex and dominant version of the DOS attack in which many attacking systems called zombies are involved. In DDOS attacks, many computers start executing DOS attacks on the same target server. As the DOS attack is spread over a large group of computers, it is known as a distributed denial of service attack.

To implement a DDOS attack as shown in figure 1, attackers use a zombie network, which is a group of infected computers on which the attacker has silently installed the DOS attacking tool [1]. Whenever the attacker wants to carry out a DDOS attack, he can employ all the computers on the ZOMBIE network to perform the attack.

In a simple word, when a server system is being flooded from fake requests coming from multiple sources (potentially hundreds of thousands), it is known as a DDOS attack [2]. In a situation like this, blocking a single or few IP addresses will not stop the attack. The more members of the computer in the zombie network, the more powerful the attack. For creating the zombie network, hackers generally use a Trojan [3].

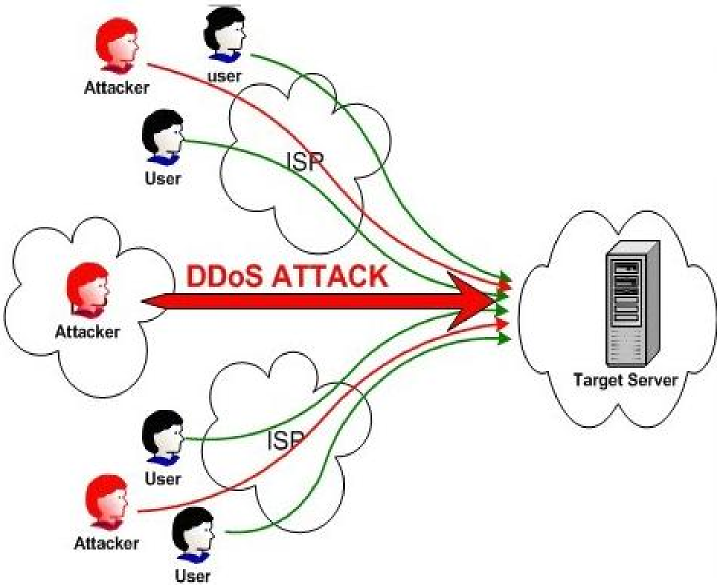


Figure 1: Distributed Denial of Service Attack [2]

In general, the purpose of a DDoS attack is to bring the service of a server to a halt and crash the website. The duration for which the DDoS attack will last depends on the fact that the attack is on the network layer or application layer [4]. The Network layer attack lasts for a maximum of 48 to 49 hours. Application layer attack lasts for a maximum of 60 to 70 days [4].

There are essentially three types of DDOS attacks:

1. Application-layer DDOS attack
2. Protocol DOS attack
3. Volume-based DDOS attack

a) **Application layer DDOS attack:** Application-layer DDOS attacks are attacks that are targeted at Windows, OpenBSD, Apache, or other software weaknesses to perform the attack and collapse the server.

b) **Protocol DDOS attack:** A protocol DDOS attacks is a DOS attack that is perpetrated at the protocol level. This category comprises of Synflood, Ping of Death, and many more.

c) **Volume-based DDOS attack**: This type of attack consist of ICMP floods, UDP floods, and other kinds of floods performed by the use of spoofed packets.

There are many tools obtainable for free that can be used to flood a server and perform an attack. A few tools also support a zombie network to execute DDOS attacks. This paper has compiled a few freely available DOS attacking tools.

II. DENIALS OF SERVICE ATTACK TOOLS

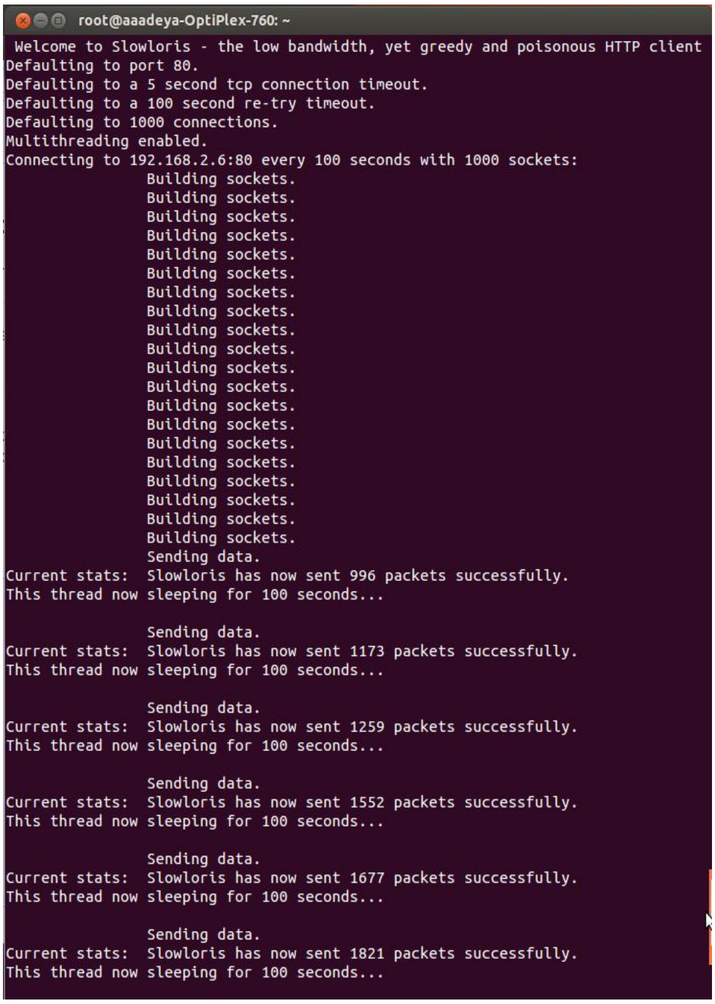
For DoS attacks to be executed there are several ways an attacker can do this. Some attackers fashion their own code that can be used to spawn malicious packet. While some use previously developed and available tools with graphical user interface (GUI). The latter technique was adopted in this study. Different DoS tools can be used to initiate an attack against the Apache web server. Some of the tools used are elucidated below;

A. SLOWLORIS

Slowloris is a packet generator, which holds connections open by constantly, sending HTTP partial requests to the target (server in this case). Successive headers are sent intermittently to keep the socket momentarily open [5]. Through this means server processes can be halted, which makes it difficult for legitimate users to access the server. Slowloris performs DoS attacks by initiating slow and partial HTTP requests which keep the IP sockets open on the victim and ultimately overwhelms all the available network ports on the server. For slowloris to function well it requires Perl, the best platform to run it is on Linux. To launch an attack, all that you need is the URL or IP address of the victim. The command below can be used to launch an attack using slowloris;

./slowloris pl –dns 192.168.2.6

Figure 2 below represents a typical slowloris in operation. In the screenshot, slowloris tries to connect with the server (192.168.2.6) on port 80.



root@aaadeya-OptiPlex-760: ~

```
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 192.168.2.6:80 every 100 seconds with 1000 sockets:
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Sending data.
Current stats:  Slowloris has now sent 996 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1173 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1259 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1552 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1677 packets successfully.
This thread now sleeping for 100 seconds...

                Sending data.
Current stats:  Slowloris has now sent 1821 packets successfully.
This thread now sleeping for 100 seconds...
```

Figure 2: Slowloris Launching attack.

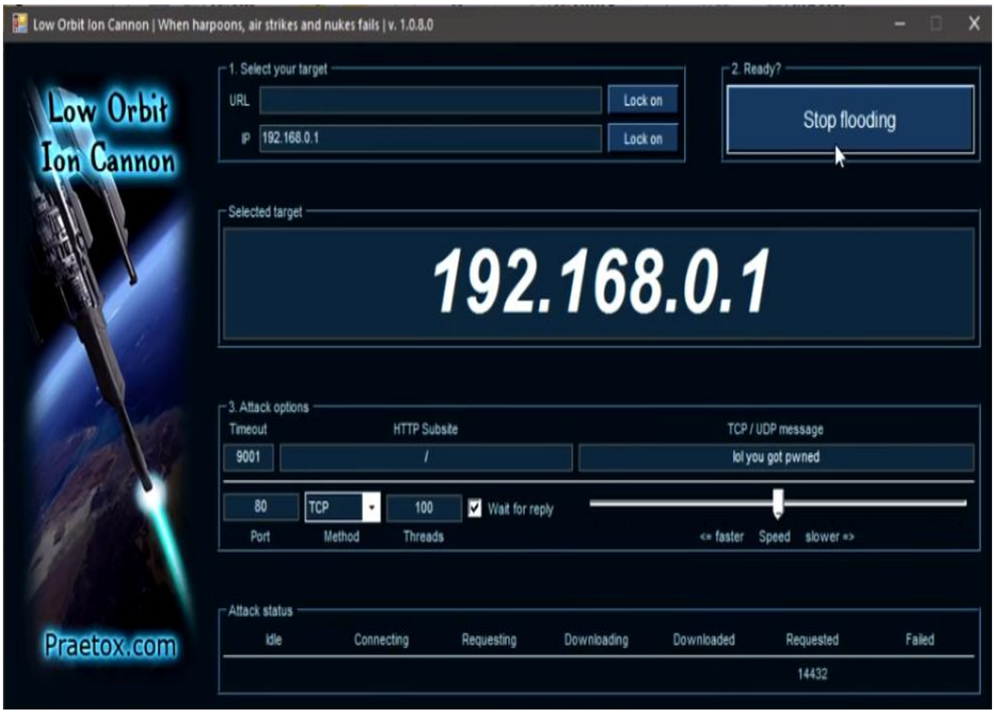
When the connection was established, at first slowlories was able to send 996 packets successfully. Subsequently, the number of packets increased gradually which is an indication of the DoS attack. During the period of this attack, other legitimate users on the network were unable to or find it difficult to connect to the server.

B. LOW ORBIT ION CANNON (LOIC)

Low Orbit Ion Cannon (LOIC) “The LOIC was originally developed by Praetox Technologies as a stress testing application before becoming available within the public domain” [8]. LOIC can be used to send a large number of UDP, TCP or HTTP requests to a host (Server); this makes the server to become unreachable to other legitimate users. It is one of the simplest DoS attack tools to use, it does not require any form of training, and it consists of a graphical user interface where details (IP address or the URL) of the target are entered and the type of attack is selected. In this study, the IP address (192.168.0.1) of the server is used, since a simple Apache web-server is installed (no URL) [5].

As stated earlier, LOIC can be used to launch 3 types of attack, these attacks are; TCP, UDP, and HTTP. From the LOIC GUI as shown in figure 3; you select the type of attack you want to launch against the server. As shown in the figure below, other forms of options to select include threads, port, TCP and UDP messages. When an attack is launched with LOIC, it opens multiple connections to the target and continuously sends TCP/UDP messages, after some time, the server becomes overwhelmed with the request which makes the server not to respond to legitimate requests.

One thing that is worthy of note is the fact that LOIC does nothing to hide the attacker’s IP address. If you are planning to use LOIC to carry out a DOS attack, reconsider. Using a proxy will not help you because it will hit the proxy server, not the target server. So using this tool against a server can create trouble for the attacker.



URL
IP 192.168.0.1

192.168.0.1

Timeout 9001
HTTP Subsite /
TCP / UDP message lol you got pwned
Port 80
Method TCP
Threads 100
☑ Wait for reply

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					14432	

Figure 3: Graphical User Interface of LOIC.

C. XOIC

XOIC is another good DOS attacking tool. It accomplishes a DOS attack on any server with a user-selected protocol, an IP address and a user-selected port. Developers of XOIC argue that XOIC is more potent than LOIC in several ways. Like LOIC, it comes with a user-friendly and easy-to-use GUI as shown in figure 4, so a novice can easily use this tool to carry out a DOS attack on a website or server.

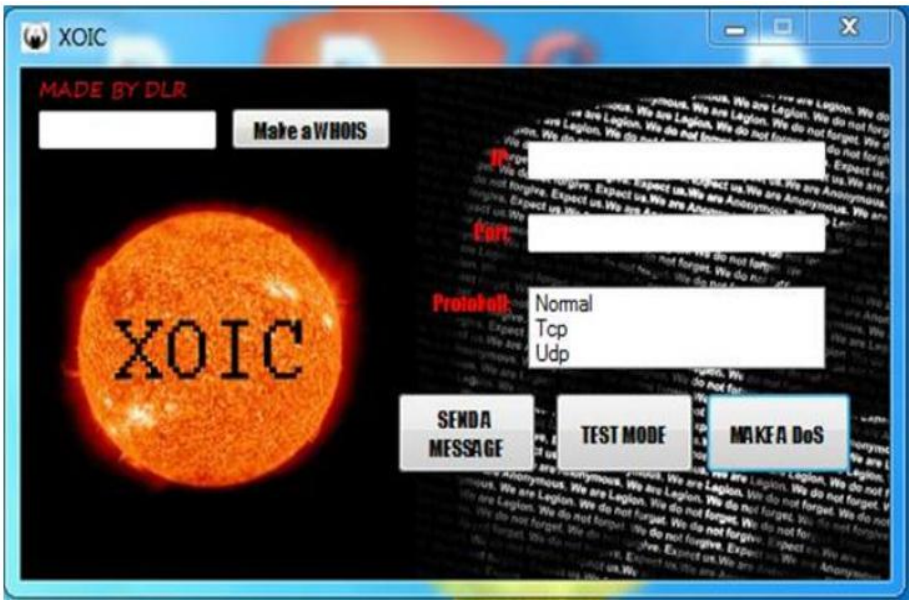


Figure 4: XOIC Graphical User Interface [4]

Generally, XOIC can be used to execute three types of attacks: test mode, normal DOS attack mode and DOS attack mode that comes with a TCP/HTTP/UDP/ICMP Message. It is an efficient tool and can be used against small websites.

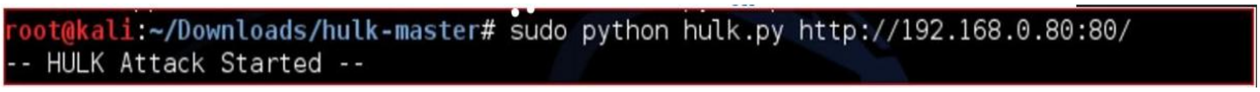
D. HULK (HTTP Unbearable Load King)

Hulk is a web server DoS tool developed for research purposes [4]. It attacks web server by generating a volume of distinctive and disguised traffic. Traffic generated by hulk also bypass caching engines and hits the server's direct resource pool. This tool is used to test network device like a firewall [8]

How to use hulk:

#sudo python hulk.py <url address>
#sudo python hulk.py http://<IP>:<PortNo>/

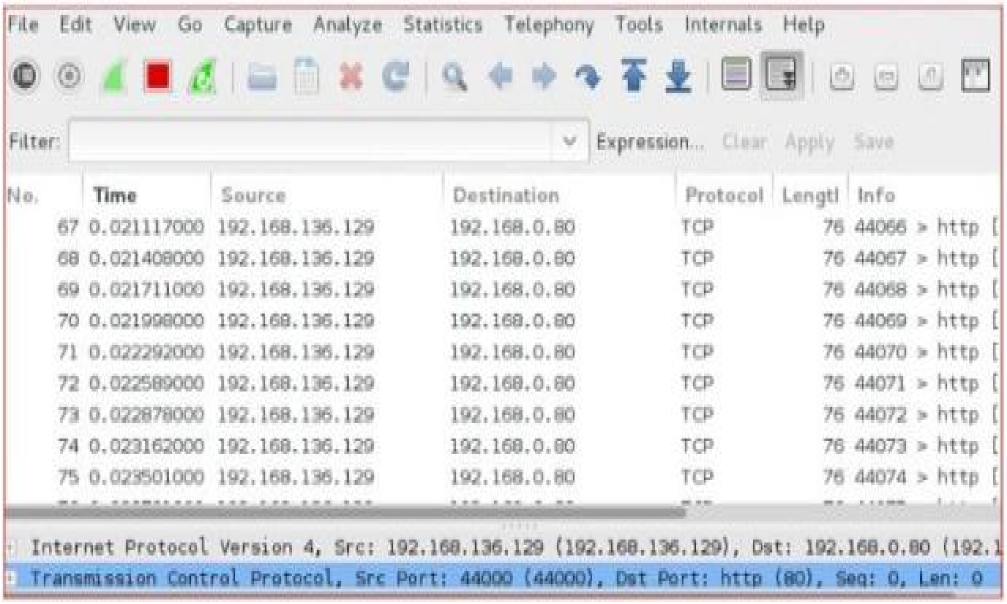
#sudo python hulk.py http://192.168.0.80:80/ as shown in figure 5 below



```
root@kali:~/Downloads/hulk-master# sudo python hulk.py http://192.168.0.80:80/
-- HULK Attack Started --
```

Figure 5: Hulk [8]

You can use Wireshark network analyzer (figure 6) to view packets
Source IP: 192.168.136.129
Destination URL: https://192.168.1.80:80/



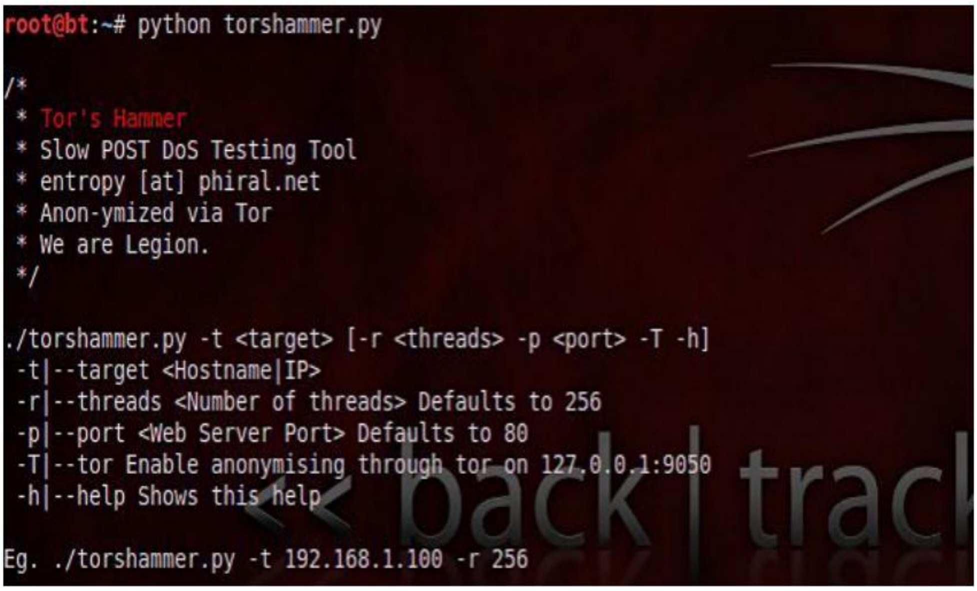
No.	Time	Source	Destination	Protocol	Lengtl	Info
67	0.021117000	192.168.136.129	192.168.0.80	TCP	76	44066 > http [
68	0.021408000	192.168.136.129	192.168.0.80	TCP	76	44067 > http [
69	0.021711000	192.168.136.129	192.168.0.80	TCP	76	44068 > http [
70	0.021998000	192.168.136.129	192.168.0.80	TCP	76	44069 > http [
71	0.022292000	192.168.136.129	192.168.0.80	TCP	76	44070 > http [
72	0.022589000	192.168.136.129	192.168.0.80	TCP	76	44071 > http [
73	0.022878000	192.168.136.129	192.168.0.80	TCP	76	44072 > http [
74	0.023162000	192.168.136.129	192.168.0.80	TCP	76	44073 > http [
75	0.023501000	192.168.136.129	192.168.0.80	TCP	76	44074 > http [

```
Internet Protocol Version 4, Src: 192.168.136.129 (192.168.136.129), Dst: 192.168.0.80 (192.1
Transmission Control Protocol, Src Port: 44000 (44000), Dst Port: http (80), Seq: 0, Len: 0
```

Figure 6: Wireshark [8]

E. TOR'S HAMMER

Tor's Hammer is a slow post DoS testing app developed in Python. It can also be run through the Tor network to be anonymized while performing the attack. It is an effective tool that can shut down Apache or IIS servers in a few seconds.



```
root@bt:~# python torshammer.py

/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
 * Anon-ymized via Tor
 * We are Legion.
 */

./torshammer.py -t <target> [-r <threads> -p <port> -T -h]
 -t|--target <Hostname|IP>
 -r|--threads <Number of threads> Defaults to 256
 -p|--port <Web Server Port> Defaults to 80
 -T|--tor Enable anonymising through tor on 127.0.0.1:9050
 -h|--help Shows this help

Eg. ./torshammer.py -t 192.168.1.100 -r 256
```

Figure 7: Tor's Hammer

F. DDoS Simulator (DDOSIM)

As the name implies, it is a tool for performing DDoS attack by reproducing several zombies. These zombie hosts create complete TCP connections to the target server, it does this by creating random IP addresses. After completing the connection, DDOSIM starts the conversation with the listening application. It can execute HTTP DDOS attack using valid and invalid requests which is similar to DC++ attack. It can also perform application layer DDOS attack.

Table 1: Summary of different DOS/DDOS attack tools [4].

DOS/DDOS attack tools	**About Attack**	**Finding(s)**
Slowloris	Send authorized HTTP traffic to the server	As it makes the attack at a slow rate, traffic can be easily detected as abnormal and can be blocked.
LOIC	UDP, TCP, and HTTP requests to the server	HIVEMIND mode will allow you to control remote LOIC systems. With the help of this, you can control other computers in the Zombie network.
XOIC	DoS attack with TCP or HTTP or UDP or ICMP message	Attack made using XOIC can be easily detected and blocked
HULK	It generates unique and obscure traffic	It may fail in hiding the identity. Traffic coming through HULK can be blocked.
Tor's Hammer	Apache & IIS server	Running the tool through the Tor network will have an added advantage as it hides your identity.
DDOSIM	Reproduce many zombie host and create complete TCP connection to the server	This tool works on Linux systems. It can attack with valid and invalid requests.

III. POSSIBLE MITIGATION TECHNIQUES

The effect of DoS/DDoS attack on the network and network resources are disruption and degradation, which in turn deny legitimate users access to the resources. DoS attacks are a growing threat on the Internet that needs greater attention. Complete eradication of DoS attack is possibly impracticable considering the present Internet infrastructure [9]. However, the approaches and strategies discussed in this paper could be collectively employed to offer various levels of DoS countermeasure techniques. Some of these countermeasure techniques are discussed in this section.

A. Firewall

A Firewall is the most widely used solution to the problems of Denial of service. This is a machine that is positioned between the internet and the local network and filters out traffic that might be detrimental to the network or the devices on the network. The firewall is typically a border control system or edge defense. The rationale behind a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside [10]. A firewall is a front line defense mechanism against intruders to enter in the system. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [11].

B. Intrusion Detection systems (IDS) and Intrusion Prevention Systems (IPS)

Another best method of detecting and mitigating DoS in a network is by using Intrusion Detection systems (IDS) and Intrusion Prevention Systems (IPS) respectively. An Intrusion

Detection system is a form is software or hardware that inspects the incoming and outgoing traffic into or from a network and identifies any mistrustful traffic from anyone trying to gain illegal access or compromise a system.

Intrusion Detection systems (IDS) can be categorized in two ways; Misuse detection (Signature based IDS) and Anomaly Detection. In signature based IDS, the IDS gathers and analyzes the traffic and compares the information gathered against a huge database of signatures or attributes that were previously documented. While anomaly IDS compares the information gathered against an established baseline: traffic load, packet size, protocol, and port number.

C. Source address

As a network administrator, you can stipulate that user accounts may log-on only from certain workstations (with a specified IP address) or certain areas of the network (that is, domains or segments). This restriction can prevent unauthorized access to the network or the servers on the network.

D. Access Control Lists

Access control lists are sets of rules that permits or denies traffic through a device or into a network. Access lists are basically a list of denying and permitting statement. One of the major functions of ACL in a network is for security purposes. An Access list is not only used for blocking of packets, but it can also be used to maintain the network that will or will not be advertised by the dynamic routing protocols [12]. All Access list configurations are the same. The only difference is the application of the list to the router or switch interfaces (inbound or outbound). Once the lists are created, they can be applied to either inbound or outbound traffic on any interface.

E. Rate Limiting

One of the best and easiest ways to stop any form of traffic from consuming the entire link is the rate limit. Rate-limiting is a method used to mitigate the DoS attack, it is a method for reducing the impact of unwanted network traffic on the trusted network and make sure it does not affect the legitimate traffic. Instead of blocking traffic, rate-limit rather set a limit on the size of the packet and the rate of transmission from the attacker to the server. This technique is implemented by most of the Internet service providers as it demonstrates to be very effective and prevents the network from been overwhelmed with unwanted traffics. Rate limiting can turn out to be very vital when all traffic to a site cannot be blocked [13].

F. Clean Up your Systems

As an Internet user, you should also take care of your system by cleaning it up. Hackers can exploit your system and use it as part of their zombie network. So, try as much as possible to protect your system. Always keep your system operating system and anti-virus up-to-date, install the latest anti-virus and patches. Always take care while downloading and installing software. On no account should you download software from un-trusted or anonymous sources. Many websites dole out malicious software to install malware in the systems of innocent users.

IV. CONCLUSION

This piece of writing is about the denial of service attacks and tools used to execute the attack. DOS attacks are used to collapse servers and interrupt service. Sony has faced this attack for a long time and lost millions of dollars. It was a big lesson for other companies who rely on server-based income [1]. Every server administrator should put an intrusion detection and prevention in place to detect and block DDOS attacks. The availability and accessibility of free tools make it simple to execute a DOS attack against a server or website. Although most of these tools are only used for carrying out DOS attacks, a few tools support a zombie network for DDOS attacks. LOIC is one of the most used and most popular DOS attacking tools. In the past few years, it has been used many times by hackers against the big company's networks, so we can never deny the possibility of attack [1]. So, every company should take care of its infrastructures and set up a good level of protection against the DOS attack.

In this paper, we have covered the overview of DoS/DDoS problem, existing DoS/DDoS attack tools, and different DoS/DDoS countermeasure mechanisms. This offers an enhanced understanding of the problem and assists the network/security administrator to efficiently fortify his network for fighting against DoS/DDoS threat. However, more research is needed to come up with a cost-effective and most efficient detection and mitigation techniques to stop the DoS/DDoS attacks. In the meantime, adhering to simple security measures is definitely the most viable in mitigating or at least minimizing DoS/DDoS attack.

REFERENCE

[1] Pavitra Shankdhar. ”Best DOS attacks and Free DOS attacking tools”. January 2019. Retrieved from: https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref.

[2] Nirbhay Ahlawat; Chetan Sharma; , "Classification and Prevention of Distributed Denial of Service Attacks" International Journal of Engineering Science and Technologies, vol. 3, no. 1, pp. 052-060, 2011.

[3] Software engineering institute, “CERT Statistics Historical”. February 12, 2009 URL: http://www.cert.org/stats/cert_stats.html.

[4] Vijay 8 Best DDoS Attack Tools. https://www.softwaretestinghelp.com/ddos-attack-tools/April 23, 2019.

[5] R. Snake, Slowloris HTTP DoS URL:http://ckers.org/slowloris/.

[6] D. Verma, LOIC (Low Orbit Ion Cannon) – DOS attacking tool December 20, 2011 URL:http://resources.infosecinstitute.com/loic-dos-attacking-tool/.

[7] Adetoye Adeyemo, “Denial of Service Detection and Mitigation.” M. Sc. Thesis, Department of Computer Science and Electronics Engineering, University of Essex, Colchester, United Kingdom. August, 2013. Pp. 15.

[8] Hulk DDoS Tool: Complete Installation and Usage with Examples Online: https://allabouttesting.org/hulk-ddos-tool-complete-installation-usage-with-examples/ published on September 8, 2017.

[9] Adetoye Adeyemo, “Denial of Service Detection and Mitigation.” M. Sc. Thesis, Department of Computer Science and Electronics Engineering, University of Essex, Colchester, United Kingdom. August, 2013. Pp. 43.

[10] Monali S. Gaigole *et al*, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 728-735.

[11] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May 2008.

[12] Todd Lammle, “Certified Network Associate Study Guide”, Cisco, SYBEX Inc, 5th Edition 2005.

[13] Michael Glenn. "A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment," SANS Institute, August 21, 2003.