Characterization and Comparison of Distributed Denial of Service Attack Tools

Harjeet Kaur
Research Scholar,Department of CSE
SBS State Technical Campus
Ferozpur-152001,Punjab
Email:harjeet.4444@gmail.com

Sunny Behal
Asstt Professor, Department of CSE
SBS State Technical Campus
Ferozpur-152001,Punjab
Email:sunnybehal@rediffmail.com

Krishan Kumar
Asso. Professor, Department of CSE
SBS State Technical Campus
Ferozpur-152001, Punjab
Email:k.salujasbs@gmail.com

***Abstract*—Distributed Denial of Service (DDoS) attack is a prime threat for the extensively used Internet based services like e-commerce, banking, medicine, education etc. Hackers launch DDoS attacks by compromising the vulnerable systems (called bots) in order to degrade or sometimes completely disrupt these services. In recent years, DDoS attacks have been increased in strength, frequency and sophistication. Though many solutions have been proposed in literature to combat against such attacks but still defending from a DDoS attack is a challenging issue. Hackers are continuously upgrading their skills to launch diversified attacks and are developing new means to circumvent these countermeasures. The purpose of this paper is to characterize and compare the popular DDoS attack tools used by the attackers in recent times, their modus operandi and types of attacks, they launch. This would help the researcher community to handpick the appropriate DDoS attack tool for their experimentation purpose.**

I. Introduction

According to CERT [1], "A DDoS attack is a malicious attempt from multiple systems to make computer or network resources unavailable to its intended users, usually by interrupting or suspending services connected to the Internet". DDoS attacks causes unusual slow performance of network, unavailability and inability to access the particular website or a service. DDoS attacks are launched through the well organized, distributed and remotely controlled network so that compromised computers (called zombies) can be used for sending large volume of simultaneous and continuous attack requests to the target system(s). As a result, target system responds slowly or completely crashed.[2]. DDoS attacks can be launched in two distinct ways. The first way is the malformed packet attack in which malformed packets are sent to the victim to embezzle the protocols or applications running on the victim machine. The DDoS attack launched by causing the disruption in the legitimate user connectivity due to the exhaustion of bandwidth, reducing router processing capacity and network resource usage, are termed as Network layer attacks whereas the attacks launched by disruption in the legitimate user services due to the exhaustion of the server resources(e.g. CPU, memory, disk/database bandwidth, sockets, input/output bandwidth) are termed as Application layer attacks. In recent years, DDoS attacks have been increased in strength, frequency and sophistication. [3], [4], [5], [6]. The attackers are the skilled persons continuously modifying their modus operandi and using latest technologies to launch diversified DDoS attacks. Although, many solutions have been proposed by the researchers to detect, prevent or mitigate DDoS attacks, but still attackers are persistently developing new methods and means to circumvent these countermeasures. [7], [8], [9], [10], [11]. Attackers use advanced methods and tools to launch DDoS attacks which leads to the huge revenue and infrastructure losses.[12]. In the recent survey conducted by the Akamai's Technologies, the number of DDoS attacks in Q1 of 2015 are increased by 35 percent as compared to Q1 of previous year[12]. A recent report from Arbor Networks indicates that the traffic volume of DDoS attack has been exponentially increased to around 400 Gbps which is 18 percent greater than was in the year 2014.[13] In july 2015, a group of hackers performed DDoS attacks on the playstation networks and disney infinity leads to the huge losses.[14]

The goal of this paper is to highlight the key features of the DDoS attack tools used by the attackers to launch DDoS attacks like their modus operandi, the type of protocol or operating system vulnerability they exploit etc. A comprehensive characterization of DDoS attack tools is provided along with the comparison of popular DDoS attack tools used by attackers in recent times. Further, technical details about attack tools and is provided with reference to the experimenters so that they can choose the appropriate DDoS attack tool or traffic generators for their experimentation purpose. This detailed information can then be use by the researchers for providing better solution to the ever growing DDoS problem.

In the literature, there are several surveys on the characterization and comparison of the DDoS attack tools.[5], [7], [15], [16] For example, Mirkovic[2001],Specht[2004],Kumar[2009] presented taxonomy of DDoS attacks and Defenses.[5], [17], [18] Hoque[2014] provide taxonomy of DDoS attacks and key features of DDoS attack tools. [16]. Inspite of these surveys, a comprehensive solution to DDoS attacks have not been formulated. What is lacking in the literature is the detailed comparison based on the key features of the DDoS attack tools so that an integrated solution can be generated. This survey provides the detailed characterization and comparison of DDoS attack tools.

This paper is organized as follows: section 2 describes the DDoS attack architecture models(Agent-Handler model and

978-1-4673-7910-6/15/$31.00 ©2015 IEEE

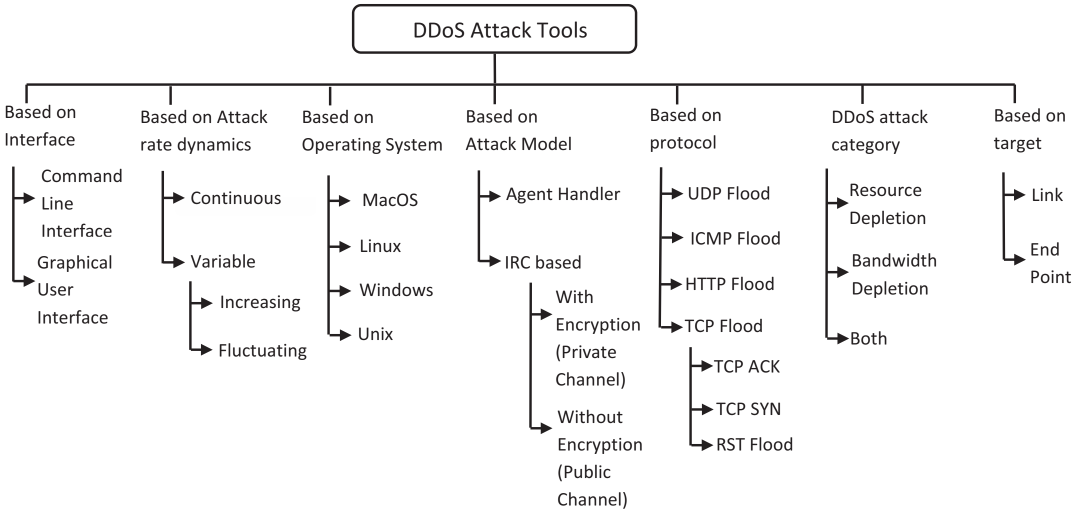

Fig. 1. Taxonomy of DDOS Attack tools

IRC-based model) and types of DDoS attacks, section 3 presents the taxonomy of DDoS attack tools and description of their attributes, section 4 emphasizes on the comparative study of the DDoS attack tools based upon their prime features, section 5 concludes the paper.

II. DDoS Architecture and DDoS attacks

This section introduce the architecture model of the DDoS attacks (i.e. the Agent-Handler model and IRC-based model)and the categorization of DDoS attacks based on the bandwidth and resource depletion. The **Agent-Handler model** of a DDoS attack comprised of client which is the main attacker, handlers are the software packages located throughout the internet and agents are the zombies which are used to launch attack.[5] The **IRC-based model** of a DDoS attack architecture uses the Internet relay chat communication channel instead of using a handler program which makes tracking the attack packets more difficult. IRC server provides an ability to handle large volumes of traffic and need not to maintain a list of the agents.[5]
There are a wide variety of DDoS attacks which can be classified as bandwidth depletion(aimed to generate the unwanted traffic in the victim network prevents the legitimate users unable to reach the victim) and resource depletion(aimed to take over the resources of the victim leads to the unavailability of the resources).[19], [20], [21], [22] On the basis of this category of DDoS attacks, attackers categorize number of DDoS attack tools to launch attacks.

III. Taxonomy of DDoS attack tools

This section introduce the taxonomy of the DDoS attack tools based on the identified attributes i.e. type of interface, attack rate dynamics, target operating system, attack model, protocols used, DDoS attack category and target area.[3], [17], [23], [24], [25] These attributes along with the explanation of DDoS attack tools as shown in Fig. 1

1) ***Type of Interface used*** :- The interfaces used by the DDoS attack tools can be either command line interface or graphical user interface. Goldeneye, trinoo, shaft etc are the examples of command line interface and hoic, udp flooder, xoic etc are the examples of graphical user interface.

2) ***Attack rate dynamics*** :- Depending upon the attack rate dynamics, attack tools can either generate the continuous attack traffic(no variations in sending attack request) rate and variable attack rate(tool can vary the attack rate to avoid the detection which can be the increasing rate and fluctuating rate).

3) ***Operating System Supported*** :- DDoS attack tools are designed to support the various operating systems. DDoS agent or handler code can be designed to work on any OS such as unix, linux, solaris or windows. Since the handler code is located at the ISP site or corporate site and is designed to support OS(unix, linux, solaris).

4) ***Attack model*** :- DDoS attack tools can also be categorized as the Agent-Handler and IRC based. Agent-Handler is single tier master-slave and can use encryption either between handler-agent or client-handler. The IRC system can have encryption at private

channel and no encryption at public channel.

5) ***Protocol*** :- Protocols can be used for flood attacks and communication between the agent-handler, handler-client and client-agent. Flood attacks are UDP, ICMP (ICMP ECHO request and ICMP ECHO reply), HTTP, TCP (TCP-SYN, TCP-ACK and RST-flood) flood attacks.

6) ***DDoS attack category*** :- The consequence of the DDoS attack is the unavailability of the resources and bandwidth. Hence the attackers designed DDoS attack tools in order to exhaust resources and bandwidth of the victim server.

7) ***Target area*** :- DDoS attacks can either congest the link or end point. So, DDoS attack tools are typically designed for the congestion at the link level(congestion at the victim network) or at the end point level(congestion at the victim server).

IV. DDoS attack tool and their comparison

In this section, comparison between the attack tools is shown in table:1 which is based on the key features e.g. impact of attack which cause destruction either at bandwidth or resource level, scope of tool, type of attack launched, support of operating systems, encryption used by the attacker, implementation language etc.[26], [27], [28] It has been investigated that all DDoS attack tools follow the generalized architecture given in [5]

1) *Stacheldraht* :- A C-based DDoS tool can create the ICMP flood, SYN flood, UDP flood and Smurf style attack to the target. It has the capability to congest the link and spoof the IP address. It can run on the linux and the solaris 2.1. [29], [64]

2) *TFN* :- TFN (tribe flood network) which can generate the multiple attacks so called the ”Son Of Trinoo”. It is the CLI based which executes on the windows, linux etc. It is written in the C language that has the attack architecture similar to the handler-agent model.[30], [64]

3) *Trinity* :- Trinity launches UDP, fragment, SYN, RST, random, flags and null flood requests that leads to the endpoint resource exhaustion and link congestion. This tool uses the encrypted format and has the command line user interface that is compatible to execute only on the linux platform.[31], [64]

4) *Bubonic* :- A DoS attempt to exploit or victimize the windows2000 machine by randomly sending a huge volume of the TCP packets with the random settings to increase the load on the machines which leads the machine to a crash. Random settings involves the setting of random IP addresses and random port number.[56]

5) *Jolt* :- A DoS attack tool sends a large number of ICMP packets in order to target the victim machine running on the windows 95 or NT so that the victim machine fails to reassemble them for use. However, this kind of attack do not cause any drastic damage to the victim system, and the machine is still in the state, to be recovered.[55]

6) *Mstream* :- A C-based DDoS attack tool has ability to forge the source addresses. It creates the TCP ACK flood and TCP RST flood requests to the target server. Both of these requests can exhaust the network resources and consumes bandwidth of the victim server.[32], [65]

7) *Shaft* :- Shaft provides statistics for TCP, UDP and ICMP flooding attacks and helps the attackers to identify the victim machine status (either completely down or alive) or to decide on the termination of zombies in addition to the attack.[33], [66]

8) *Targa* :- Targa is the DoS attack tool which is the collection of the 16 different programs of DoS. These attacks can be launched individually as well as in the group also. These can also damage the whole network in the instant.[57]

9) *Trinoo* :- An effective DDoS attack tool, that uses a master host and several broadcast hosts. Master host instructs the various broadcast hosts to launch the attack. An Application layer attack tool that has the capability to deplete the resources and leverages the bandwidth of the victim network.[34], [64]

10) *Blast20* :- A DOS attack tool which is also called as the TCP service stress tool is able to identify the potential weaknesses in the network servers instantly. The parameters involved to launch attack are target IP address, start size and end size of the packet.[56]

11) *Crazy Pinger* :- A DoS attack tool which can launch attack by sending a large volume of ICMP packets to the victim machine or to the large remote network. This kind of tool is easy to use and is effective over the multiple platforms.[58]

12) *Kaiten* :- A DDoS attack tool which can launch multiple attacks, viz., UDP flood, TCP flood, SYN flood and PUSH+SYN flood. It uses random source IP addresses. Its architecture is the IRC based.[62]

13) *Knight* :- An IRC-based tool can launch multiple DDoS attacks to create SYN flood, UDP flood and urgent pointer flood on windows machines. An IRC based tool that can destroy the resources and the bandwidth of the victim system.[20], [35]

TABLE I
COMPARATIVE FEATURES OF DDOS ATTACK TOOLS

Year of the tool	Name of attack tool(Source to download)	Target Impact	Scope	Type of Attack Launched	Operating System supported	Number of Zombies	whether makes botnets? (yes/no)	Encryption (yes/no)	Ip Spoofing (yes/no)	Implementation Language	Interface	Architecture Model
1999	Stacheldraht [29]	Bandwidth, Resource Depletion	DoS, DDoS	icmp,udp	linux, solaris2.x	Multiple	yes	yes	yes	C	CLI	Agent based
1999	TFN(Tribe flood network)[30]	Bandwidth, Resource Depletion	DDoS	tcp,udp, icmp	windows, linux ,solaris	Multiple	yes	no	yes	C	CLI	Agent based
1999	Trinity[31]	bandwidth, resource Depletion	DoS, DDoS	tcp,udp	linux	Multiple	yes	no	no	-	CLI	IRC based
2000	Bubonic[56]	Resource and Bandwidth Depletion	DoS	tcp	windows, linux, unix	single	no	no	no	C	-	-
2000	Jolt[55]	Resource Depletion	DoS	icmp	window95, windowsNT	Single	no	no	yes	C	CLI	-
2000	Mstream[32]	Bandwidth Depletion	DoS, DDoS	tcp,udp, icmp	linux, windows	Multiple	yes	no	yes	C	CLI	Agent based
2000	Shaft[33]	Bandwidth, Resource Depletion	DoS, DDoS	udp,icmp ,tcp	linux, unix	Multiple	yes	no	yes	-	CLI	Agent based
2000	Targa[57]	Resource and Bandwidth Depletion	DoS	tcp,udp,icmp	linux	Single	yes	no	yes	C	-	-
2000	Trinoo[34]	Bandwidth Depletion	DDoS	udp,tcp ,http	linux ,solaris	Multiple	yes	yes	no	C	CLI	Agent based
2001	Blast20[56]	Resource Depletion	DoS	tcp	windows , linux, unix	Single	no	-	-	-	CLI	-
2001	Crazy Pinger[58]	Resource and Bandwidth Depletion	DoS	icmp	windows, linux, unix	Single	no	no	yes	-	GUI	-
2001	Kaiten[62]	Resource and Bandwidth Depletion	DDoS	tcp,udp	windows	Multiple	Yes	no	no	-	CLI	IRC based
2001	Knight[35]	Bandwidth, Resource Depletion	DDoS	tcp,udp	windows	Mutiple	yes	no	-	C	CLI	IRC based
2003	Nemsey[60]	Bandwidth Depletion	DoS	tcp	windows	Single	no	no	no	no	GUI	-
2005	FSMax[59]	Resource Depletion	DoS	-	windows	Single	no	no	no	-	CLI	-
2005	Hping[36]	Resource Depletion	DoS	icmp, udp,tcp	linux, windows	Single	no	no	yes	TCL	CLI	-
2007	Black Energy[37]	Resource, Bandwidth Depletion	DDoS	tcp,udp, icmp,http	linux	Multiple	yes	no	-	-	CLI	IRC based
2007	Hgod[63]	Resource and Bandwidth Depletion	DDoS	tcp,udp,icmp	windows	Multiple	-	no	yes	-	CLI	IRC based
2007	Panther[61]	Bandwidth Depletion	DoS	icmp,udp	-	Single	no	-	-	-	-	-
2007	RefRef[56]	Resource Depletion	DDoS	-	windows	Multiple	-	no	no	perl	CLI	IRC based
2008	LOIC[38]	Resource Depletion	DoS, DDoS	tcp,udp, icmp,http	linux,mac os,windows ,android	Multiple	yes	no	no	C-Sharp	GUI	IRC based
2008	UDP Flooder[39]	Bandwidth Depletion	DoS	udp	windows	-	-	no	yes	-	GUI	IRC based
2009	DDOSIM[40]	Resource Depletion	DDoS	tcp,smtp ,http,udp	linux	Multiple	yes	no	no	C++	CLI	-
2009	Slowloris[41]	Bandwidth, Resource Depletion	DoS	http	windows, linux	Single	no	no	no	Perl	GUI and CLI	-
2009	TOR's hammer[42]	Resource, Bandwidth Depletion	DoS, DDoS	http	unix, linux, macos	Multiple	yes	no	no	Python	CLI	Agent based
2010	Davoset[43]	-	DoS, DDoS	http	linux	Multiple	yes	no	no	Perl	CLI	-
2010	Owasp Http Dos Post[44]	Resource Depletion	DoS	http	windows	Single	no	no	no	Python	GUI	-
2010	Pyloris[45]	Resource Depletion	DoS, DDoS	tcp,imap ,udp,smtp ,http,ftp, telnet	linux, windows, macos	Multiple	yes	no	yes	Python	CLI	IRC based
2010	XOIC[46]	Resource Depletion	DoS, DDoS	udp,tcp, icmp	windows	Multiple	yes	no	no	C-Sharp	GUI	IRC based
2011	Aldi Botnet[47]	Resource Depletion	DDoS	http,tcp	windows	Multiple	yes	no	no	-	GUI	Web based
2011	R-U DEAD - YET[48]	Resource Depletion	DoS, DDoS	http	linux	Single	no	no	yes	Python	CLI	-
2011	SSL DoS[49]	Resource Depletion	DoS	tcp	windows , unix	Single	no	-	-	-	-	-
2012	GoldenEye[50]	Resource Depletion	DoS	http	Linux, Windows, MAC	Single	no	no	no	Python	CLI	-
2012	HOIC[51]	Resource Depletion	DDoS	http	windows	Multiple	yes	no	no	Basic	GUI	-
2012	HULK[52]	Resource Depletion	DoS, DDoS	http	linux, windows	Single	no	no	no	Python	CLI	-
-	Silent-Ddoser[53], [54]	-	DDoS	udp,tcp, http	windows	Multiple	yes	yes	no	VB.net	GUI	IRC based

14) *Nemsey* :- A DoS attack tool whose presence specifies the computer is insecure and infected with the malicious software. It attempts to launch an attack with a specified number of packets of specified sizes.[60]

15) *FSMax* :- A DoS attack tool which can be used to test the stress of the network and to test the server for case of buffer overflows which may be exploited during attack, text file is accepted as the input which is executed through a sequence of tests based on the input.[59]

16) *Hping* :- Hping3 is the tool works like Hping2 that can handle the random packet size and the fragmentations. Hping2 performs the firewall rule testing, port scanning and protocol based network performance testing. A tool that cannot form zombies and can degrade the resources of the victim.[36], [67]

17) *Black Energy* :- Black energy is the simple and powerful DDoS attack tool and a well known cybercrime toolkit. This tool continues to be widely used to deny services for commercial websites and targets the critical energy infrastructure.[37]

18) *Hgod* :- This tool is the windows XP based tool which can spoof the source IPs and specifies protocols and the port numbers during the attack. It is used for the TCP SYN flooding attack.[63]

19) *Panther* :- A UDP based DoS attack tool that can flood the specified IP at a particular port number. It takes IP address as the input parameter to launch the attack. This tool is the windows based.[61]

20) *RefRef* :- A DDoS attack tool which is used to exploit existing SQL injection vulnerabilities. It sends the SQL malformed queries which are carrying payloads that force the servers to exploit their own resources. This tool works with the perl compiler in order to launch attack.[56]

21) *Loic* :- An open source network testing and DoS attack tool developed by Praetox Technologies. Loic was used by 4chan during Project Chanology to attack websites from the Church of Scientology, once again a successful attack on the recording of Industry Association of America's website in October 2010.[38]

22) *UDP Flooder* :- UDP flooder is the port scanner and has user friendly graphical user interface that can target the random ports and random packet size. UDP-Flooder came into existence in the year 2008 which has the capability to deplete the bandwidth of the victim server. [39]

23) *Ddosim* :- A DDoS attack tool that uses the random IP addresses to stimulate several zombies with full TCP connection. It generates the HTTP-GET flood attack to target random IP addresses and random ports.[40], [68]

24) *Slowloris* :- Slowloris attack tool creates the TCP SYN requests to the target victim. During the Iranian presidential election in 2009, Slowloris arose as a prominent tool used to leverage DoS attacks against sites run by the Iranian government.[41], [69]

25) *Tor's Hammer* :- A python based slow post DoS testing tool that runs through TOR network. It uses random source IP address making difficult to trace back the source machine of the attacker. This tool that can deplete the bandwidth and resources of the victim server.[42]

26) *Davoset* :- Davoset is a command line tool for conducting DDoS attacks on the sites via Abuse of functionality and XML external entities vulnerabilities at sites for attack on other sites (including DoS and DDoS attacks).[43]

27) *Owasp DoS http post* :- An open web application software project for testing performance, availability and capacity planning of web application. Slow HTTP POST attack requests are sent to the victim and maintain SSL half connection with the victim.[44], [68]

28) *Pyloris* :- Pyloris is the scriptable tool for testing a service level of vulnerability to a particular class of Denial of Service. It uses the methods of Slowloris and is used to test the server's readiness to withstand Botnet DDoS attacks.[45], [68]

29) *Xoic* :- Xoic can perform the DDoS attack on any server with an IP address, a user-selected port and a user-selected protocol. It seems to be more powerful than the Loic. DDoS attacks can be performed with TCP, HTTP, UDP, ICMP packet messages.[46]

30) *Aldi Botnet* :- Aldi botnet is a newer inexpensive DDoS bot that is growing in the wild. Arbor company on September 30,2011 suggests that there are at least 50 distinct aldi botnets that have been seen in the wild with 44 unique command and control points. Active botnets are seen in Russia, Ukraine, US, Germany.[47]

31) *R-U-dead-Yet* :- Rudy is the python based slow attack tool to crash the web server. It has two modes, one is the interactive menu mode and another is the unattended configuration based execution mode. A python based tool that can launch attack in order to deplete the resources of the victim server.[48], [69]

32) *SSL DoS* :- A Windows tool that can cause denial of service attack without creating the botnets. This tool can be executed on the both windows and Linux, is more effective and powerful. This tool came in the year 2011. It can launch the network layer attacks.[49]

33) *Golden-Eye* :- Golden-Eye DoS test tool is the multi threaded python based that performs the http flood attack. Attack vector exploitation can be done by HTTP keep alive+no cache. It neither encrypt the attack packets nor spoof the IP addresses of attacking machines. This tool can execute on the Windows, Linux, MACOS.[50], [68], [70]

34) *Hoic* :- High speed, multi threaded attack tool and has the capability to flood upto 256 websites at once. HTTP GET flood and POST requests are sent to the target server. Anonymous was the first group to utilize it and launch attack against the website of the US department of justice.[51]

35) *Hulk* :- HTTP unbearable load king has ability to take down the server in a minute as it directly affects the server's load. It generates TCP SYN flood and multi threaded HTTP GET flood requests.It can hide the actual user agent. It has the ability to send the different patterns of attack requests that can obfuscate the referrer for each request.[52], [71]

36) *Silent ddoser* :- Silent ddoser can create UDP, SYN and HTTP flood requests to the target victim. It has ability to update the bots on the botnet at ongoing attack. It utilizes triple-DES, RC4 encryption and has IPV6 capabilities with password stealing function. It is a windows tool which has graphical user interface.[53], [54]

A wide variety of DDoS attack tools are available on the internet. Most of them are very powerful and destructive, these can easily crash the network and web applications in terms of bandwidth and resource depletion. Out of these attack tools black energy, loic, hoic, r-u-dead-yet, hulk have support for http protocol to constructs the attack packets whereas other tools like ssl-DoS, targa, jolt etc do not have any support for http protocol. Although tfn, trinoo, stacheldrath, shaft, mstream, trinity have capability to launch DDoS attacks but these are not much powerful as compared to other attack tools. The parameters required to launch an attack vary with the type of attack tool used. The year-wise comparison shows the drastic change in the features of attack tools. Using these attack tools in the public network causes crime.

V. Conclusion

DDoS is the severe, long lasting problem that makes the service unavailable to the legitimate users and cause high revenue and financial loss to the numerous applications including communication, banking, medicine and research. To counter such attacks, number of taxonomies of the DDoS attacks and the countermeasures are proposed. Such taxonomies of DDoS attacks provides the positive benefit to the researchers in terms of the characteristic features to gain broad understanding of the attack. The previously mentioned taxonomies are failed to provide an appropriate solution for the DDoS problem because individual solutions are incomplete in themselves. The requirement is the internet community must be collaborative like the attackers community which performs attack over the victim server. Since the attackers cooperatively exchange the attack code and information about the vulnerable machines. The organization of the agent machines coordinated into the network to acquire the immense power and survivability.

This kind of cooperative strategy must be followed by the internet community to counter the attacks. Good DDoS attack tool taxonomy will facilitate the communication and offers a common language to the community to provide solutions came from discussions. These identifies the various weaknesses which could be removed by providing additional mechanisms. In the same way, the research community must develop the common benchmarks and the metrics to evaluate the efficiency of the various defensive systems. With the detailed study of the attack tools, type of DDoS attacks can be distinguished and seems to be powerful and efficient. This paper concludes with the numerous features of the attack tools that will help to get appropriate attack tool for their experimentation purpose only when the research community cooperatively and coordinately find the solution of DDoS problem.

References

[1] "certorg," 2015. [Online]. Available: http://www.cert.org/

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 4, pp. 2046–2069, 2013.

[3] J. Mirkovic, S. Fahmy, P. Reiher, and R. K. Thomas, "How to test dos defenses," in *Cybersecurity Applications & Technology Conference For Homeland Security*. IEEE, 2009, pp. 103–117.

[4] A. Hussain, S. Schwab, R. Thomas, S. Fahmy, and J. Mirkovic, "Ddos experiment methodology," in *Proceedings of the DETER Community Workshop on Cyber Security Experimentation*, vol. 8, 2006.

[5] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures." in *ISCA PDCS*, 2004, pp. 543–550.

[6] S. Behal and K. Kumar, "An experimental analysis for malware detection using extrusions," in *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on*. IEEE, 2011, pp. 474–478.

[7] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting distributed denial of service attacks: methods, tools and future directions," *The Computer Journal*, p. bxt031, 2013.

[8] S. Behal, A. S. Brar, and K. Kumar, "Signature-based botnet detection and prevention," *http://www. rimtengg. com/iscet/proceedings/pdfs/advcom p/148. pdf*, 2010.

[9] N. Kaur and S. Behal, “P2p-bds: Peer-2-peer botnet detection system,” 2006.

[10] V. Bukac, “Traffic characteristics of common dos tools,” 2014.

[11] A. Hussain, J. Heidemann, and C. Papadopoulos, “A framework for classifying denial of service attacks,” in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2003, pp. 99–110.

[12] “Akamai,” 2015. [Online]. Available: http://www.securityweek.com/ddos-attacks-spiked-q1-2015-akamai

[13] “Arbor,” 2015. [Online]. Available: http://www.scmagazine.com/largest-ddos-detected-in-q1-report-says/article/411648/

[14] “Playstation,” 2015. [Online]. Available: http://www.wsbtv.com/videos/news/psn-down-after-ddos-attack-news-flash/vCpxR2/

[15] M. C. M. Patel and A. P. V. H. Borisagar, “Survey on taxonomy of ddos attacks with impact and mitigation techniques,” in *International Journal of Engineering Research and Technology*, vol. 1, no. 9 (November-2012). ESRSA Publications, 2012.

[16] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. Bhattacharyya, and J. K. Kalita, “Network attacks: Taxonomy, tools and systems,” *Journal of Network and Computer Applications*, vol. 40, pp. 307–324, 2014.

[17] J. Mirkovic, J. Martin, and A. Peter Reiher, “Taxonomy of ddos attacks and ddos defense mechanisms computer science department university of california,” Los Angeles Technical report, Tech. Rep., 2001.

[18] P. A. R. Kumar and S. Selvakumar, “Distributed denial-of-service (ddos) threat in collaborative environment-a survey on ddos attack tools and traceback mechanisms,” in *Advance Computing Conference, 2009. IACC 2009. IEEE International*. IEEE, 2009, pp. 1275–1280.

[19] A. Srivastava, B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, “A recent survey on ddos attacks and defense mechanisms,” in *Advances in Parallel Distributed Computing*. Springer, 2011, pp. 570–580.

[20] C. Douligeris and A. Mitrokotsa, “Ddos attacks and defense mechanisms: classification and state-of-the-art,” *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004.

[21] R. K. Chang, “Defending against flooding-based distributed denial-of-service attacks: a tutorial,” *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 42–51, 2002.

[22] Y. Chen, K. Hwang, and W.-S. Ku, “Collaborative detection of ddos attacks over multiple network domains,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 18, no. 12, pp. 1649–1662, 2007.

[23] S. Ghansela, “Network security: Attacks, tools and techniques,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 419–421, 2013.

[24] M. Aamir and M. A. Zaidi, “Ddos attack and defense: Review of some traditional and current techniques,” *arXiv preprint arXiv:1401.6317*, 2014.

[25] C. Meadows, “A formal framework and evaluation method for network denial of service,” in *Computer Security Foundations Workshop, 1999. Proceedings of the 12th IEEE*. IEEE, 1999, pp. 4–13.

[26] N. Dhanjani and J. Clarke, *Network Security Tools: Writing, Hacking, and Modifying Security Tools*. ” O’Reilly Media, Inc.”, 2005.

[27] H. Debar, M. Dacier, and A. Wespi, “Towards a taxonomy of intrusion-detection systems,” *Computer Networks*, vol. 31, no. 8, pp. 805–822, 1999.

[28] J. Mirković, G. Prier, and P. Reiher, “Attacking ddos at the source,” in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*. IEEE, 2002, pp. 312–321.

[29] “Stacheldraht,” 2000. [Online]. Available: https://packetstormsecurity.com/distributed/stachel.tgz

[30] “Tfn,” 2000. [Online]. Available: http://packetstormsecurity.com/distributed/page3/

[31] “Trinity,” 2012. [Online]. Available: https://www.thebuddyforum.com/archives/70841-trinity-download-v1-6-3-4-a.html

[32] “mstream,” 2000. [Online]. Available: https://packetstormsecurity.com/files/17748/mstream.txt.html

[33] “Shaft,” 2000. [Online]. Available: https://packetstormsecurity.com/files/17137/shaftnode.txt.html

[34] “Trinoo,” 2000. [Online]. Available: https://packetstormsecurity.com/files/11215/trinoo.tgz.html

[35] “knight,” 2001. [Online]. Available: https://packetstormsecurity.com/files/23939/knight.c.html

[36] Antirez, “hping,” 2014. [Online]. Available: https://github.com/antirez/hping

[37] “Blackenergy,” 2014. [Online]. Available: http://powersource.post-gazette.com/powersource/companies/2014/11/11/BlackEnergy-spooks-nation

[38] “Loic,” 2015. [Online]. Available: http://sourceforge.net/projects/loic

[39] “Udpunicorn,” 2011. [Online]. Available: http://sourceforge.net/projects/udpunicorn

[40] “Ddosim,” 2010. [Online]. Available: http://sourceforge.net/projects/ddosim

[41] “Slowloris,” 2012. [Online]. Available: http://sourceforge.net/projects/slolorisgui

[42] “Torshammer,” 2011. [Online]. Available: http://packetstormsecurity.com/files/98831/

[43] “Davoset,” 2015. [Online]. Available: https://packetstormsecurity.com/files/132515/DAVOSET-1.2.5.html

[44] “Owasp,” 2014. [Online]. Available: https://www.owasp.org

[45] “pyloris,” 2010. [Online]. Available: http://sourceforge.net/projects/pyloris

[46] “Xoic,” 2013. [Online]. Available: http://sourceforge.net/projects/xoic

[47] “Aldibotnet,” 2012. [Online]. Available: https://asert.arbornetworks.com/ddos-tools

[48] “Rudy,” 2010. [Online]. Available: https://packetstormsecurity.com/files/95882/R-U-Dead-Yet-Denial-Of-Service-Tool.html

[49] “Ssldos,” 2011. [Online]. Available: https://www.thc.org/thc-ssl-dos/

[50] J. Seidl, “Goldeneye,” 2014. [Online]. Available: https://github.com/jseidl/goldeneye

[51] “Hoic,” 2013. [Online]. Available: http://sourceforge.net/projects/hoic/

[52] “Hulk,” 2012. [Online]. Available: https://packetstormsecurity.com/distributed

[53] “Silentddoser1,” 2012. [Online]. Available: https://asert.arbornetworks.com/ddos-tools/

[54] “Silentddoser,” 2015. [Online]. Available: http://zaxx.cba.pl/17589.html

[55] “jolt,” 2015. [Online]. Available: http://searchsecurity.techtarget.com/definition/jolt

[56] “burblast20,” 2015. [Online]. Available: http://www.softpedia.com/

[57] Mixter, “Targa,” 2009. [Online]. Available: http://wiki.cas.mcmaster.ca/index.php/Tools-for-conducting-denial-of-service-attacks

[58] “crazypinger,” 2015. [Online]. Available: http://seomagz.com/2010/03/dos-denial-of-service-attack-tools-ethical-hacking-session-3/

[59] “fsmax,” 2015. [Online]. Available: www.brothersoft.com

[60] “nemsey,” 2015. [Online]. Available: http://packetstormsecurity.org

[61] “panther,” 2015. [Online]. Available: http://www.bestspywarescanner.net

[62] “kaiten,” 2015. [Online]. Available: http://www.mcafee.com

[63] “hgod,” 2015. [Online]. Available: hhttp://www.flylib.com

[64] P. J. Criscuolo, “Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319,” DTIC Document, Tech. Rep., 2000.

[65] D. Dittrich, G. Weaver, S. Dietrich, and N. Long, “The mstreamdistributed denial of service attack tool,” *URL http://staff. washington. edu/dittrich/misc/mstream. analysis. txt*, vol. 3, 2000.

[66] S. Dietrich, N. Long, and D. Dittrich, “Analyzing distributed denial of service tools: The shaft case.” in *LISA*, 2000, pp. 329–339.

[67] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, “Denial-of-service attack-detection techniques,” *Internet Computing, IEEE*, vol. 10, no. 1, pp. 82–89, 2006.

[68] N. C. S. Iyengar, A. Banerjee, and G. Ganapathy, “A fuzzy logic based defense mechanism against distributed denial of services attack in cloud environment,” *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 6, no. 3, 2014.

[69] E. Damon, J. Dale, E. Laron, J. Mache, N. Land, and R. Weiss, “Hands-on denial of service lab exercises using slowloris and rudy,” in *Proceedings of the 2012 Information Security Curriculum Development Conference*. ACM, 2012, pp. 21–29.

[70] Z. Xu, J. Zhang, G. Gu, and Z. Lin, “Goldeneye: Efficiently and effectively unveiling malwares targeted environment,” in *Research in Attacks, Intrusions and Defenses*. Springer, 2014, pp. 22–45.

[71] A. Kapravelos, C. Grier, N. Chachra, C. Kruegel, G. Vigna, and V. Paxson, “Hulk: Eliciting malicious behavior in browser extensions,” in *Proceedings of the 23rd Usenix Security Symposium*, 2014.