DDoS Attacks Tools and Traffic Generators: A Review

Usman Ali[†], Qaiser Abbas Khan[c††], Muhammad Kashif Nazir[†††], Rao Sohail Iqbal[††††] , Hina Zafar[†††††],
[†,††,†††,†††††]Riphah College of Computing, Riphah International University, Faisalabad Campus, Pakistan
[††††]Government College University, Faisalabad

Summary
As technology increasing rapidly, cyber security threats increasing too. Denial of service or DDoS is also an online attack in which a person attack the system with flood of traffic. A DDoS consists of sending and requesting a lot of data to a server in a network, thus getting the server saturated and unable to respond to data requests that are legitimately made. Hackers continuously upgrading their skills to attack systems and to avoid system crashes and breakdown of systems need some kind of tools that we can use to prevent these attacks. This paper will discuss in detail about characteristics and comparison of tools that used for DDoS Attacks and used to generate traffic.

Keywords:
DDoS, Cyber Security, Flood of Traffic, Ddos Attack tools, Traffic generators

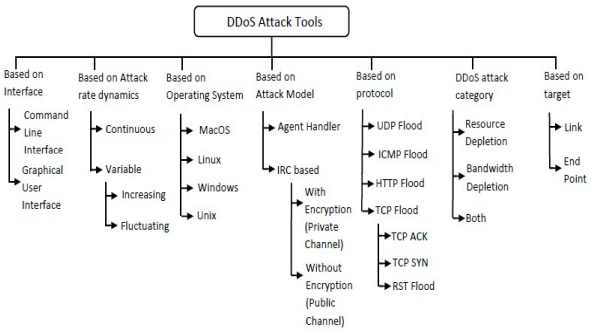

Fig. 1 DDoS Attacks Tools [6]

1. Introduction

DDoS stands for Distributed Denial of Service, which translates as a Distributed Interruption of the service, and consists of filling a site with requests until it is knocked out and made unreachable. According to the latest data from the association for information security, it is among the attacks that hit a company every five minutes along with malware and ransom-ware. Its use has decreased compared to previous years, registering 66.96%, their power has increased: the average occupied band has increased from 11 gigabits per second in 2016 to 59 Gigabits per second in 2018 [1]. DDoS attacks launch with different kind of tools that tools can slow down systems or can shut down the system. When multiple sources of computers used to destroy an online service it is called DDoS. A well-known practical example is Mirai [2] [3], a botnet created by infecting thousands of devices, which occupied the international chronicles showing what these systems are capable of doing. There are a lot of tools that an attacker can use to generate traffic and can use to attack. D. ITG [4] [5] is a very powerful tool that can generate a high number of traffic. There are many other tools that can be used into DDoS Attack.

2. DDoS Attack Tools and Comparison

2.1 Stacheldraht.

Stacheldraht is a tool that makes ICMP, UDP, Smurf, and SYN floods towards the targeting server. It consist on a CLI (Command Line Interface) and uses agent-based architecture model. It is based on C [7].

2.2 TFN

It is used to generate a different kind of attacks. It also has a name “Son of Trino” It can work on window and Linux both. It is based on C programming and use CLI. It produces DDoS attacks that have the ability to exhaust both resource and bandwidth [8] of the objective.

2.3 Trinty

This tool uses CLI base interface and generate UDP, RST, and fragment flood to destroy online services. It used encrypted format and work on Linux based platform [9].

Manuscript received November 5, 2025
Manuscript revised November 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.11.14

2.4 Jolt

It is c language based attack, worked on Windows 95 and NT. It sends ICMP Packets to destroy services. It is an old attack. However, this attack has less effect that does not cause the major damage and the machine can be recovered easily under this attack [10].

2.5 Panther

It is a window based tool that attacks a specific port number of a specific IP. It has the capability to occupy all of the victim's bandwidth machine and slow down the services of it with TCP and UDP traffic flood [10].

2.6 UDP Flooder

It is usually done to machines that run the Echo service waiting for the response of these with large packets. Users cannot ask for freedom of expression because a website is closed and at the same time limit this same freedom attacking other websites even if users disagree with their opinion. The way to solve Wikileaks problems is not to go against Visa or Mastercard, but it is to give all the diffusion to the information that has been published here [11].

2.7 DDoSim

Distributed Denial of Service attack apparatus that uses the irregular addresses of IPs to invigorate a few zombies with full TCP association. DDoSim can generate the HTTP-GET flood attack to victim arbitrary IP addresses and irregular ports. A CLI or command line interface whose usage dialect is the C++ and has the capacity to drain the resources of the targeted server.

2.8 HOIC

It is very fast, multi-strung attack instrument and it has capability to flood up to 256 sites at one time. HTTP-GET flood and POST asks for sent to the objective server. A group name Anonymous, was the first group that used this and dispatch attack against the site of the US Bureau of justice [12].

Table 1: Margin specifications

Margin	***A4 Paper***	US Letter Paper
Left	18.5 mm	14.5 mm (0.58 in)
Right	18mm	13 mm (0.51 in)

Table 1: DDoS Attack Tools Comparison

Name	**Target Impact**	**Type of Traffic Attack**	**Interface Type**	**Supported Operating Systems**
Stacheldraht	Resource & Bandwidth	TCP & UDP	CLI	Linux
TFN	Resource & Bandwidth	TCP & UDP & ICMP	CLI	Linux, Windows
Trinty	Resource & Bandwidth	TCP & UDP	CLI	Linux
Jolt	Resource	ICMP	CLI	Windows 95, NT
Panther	Bandwidth	ICMP	GUI	Windows & Linux
UDP Flooder	Bandwidth	UDP	GUI	Windows & Linux
DdoSim	Resource	Tcp, HTTP, UDP and SMTP	CLI	Linux
HOIC	Resource	HTTP	GUI	Windows

3. Traffic Generator and Comparison

It is a different kind of tools that used to generate traffic to make targeted system idle or used in denial of services.

3.1 NetPerf

It is available publically and it is open source tool that use to measure the performance of different kind of networks. It is based on c language and uses command line interface it generates transport and network layer traffic [13].

3.2 Ostinato

Open source and use python language to generate traffic with different protocols. It is also a transport and network layer traffic generator [14].

3.3 Pylot

It is also a python base open source generator. It generates the HTTP load to verify server response and generate a report. It is a multi-thread load generator and publically available.

3.4 RUDE

It is a UDP data generator that generates UDP packets and flood on a targeted machine with the help of CRUDE. CRUDE is a combination of RUDE. It is a C-based and publically available [15].

3.5 SEER

SPARTA Inc. developed it called Security experimentation environment (SEER). It is a java base generator that use to generate legitimate traffic to destroy a victim's services [16].

3.6 TCP Replay

This generator provides a reliable and efficient environment for testing different networks devices like switches, routers etc. It is a CLI based generator and generates Network layer traffic [16].

3.7 TMIX

It is embedded in the GENI platform that generates realistic traffic. It needs full TCP or one-sided TCP. It is publically available Linux base generator that generates traffic in the transport layer [14] [15].

3.8 WEBSTONE

This generator used to test the performance of HTTP in contrast to servers. It can measure the average time of connection and performance of servers. It is an application layer traffic generator and C-based [14].

. **Table 2:** Comparison of Traffic Generators

Name	Implementation Language	Traffic	GUI/ CLI	Operating Layers
NetPerf	C	SCTP, IP, UDP, TCP	CLI	Transport and Network
Ostinato	Python	TCP, ICMP, UDP	GUI	Network and Transport Layer
Pylot	Python	HTTP & HTTPS	GUI	Application layer
RUDE	C	UDP	GUI	Transport Layer
SEER	Java	TCP, UDP, HTTP, ICMP	GUI	Network/ Application & Transport
TCP Replay	C / C++	TCP IP	CLI	Network layer
TMIX	NS-2	TCP IP	CLI	Application Layer
WEBSTONE	C	HTTP	CLI	Application Layer

4. Progress on DDoS

A Security company name Cordero took a survey and find that an organization spends up to 50000$ to deal with a single attack. There is some advancement on the DDoS assault front. As per Forbes, European law enforcement as of late close down a site that sold DDoS attackers and helped dispatch them for many paying clients. The organization cautioned organizations and people to quit utilizing DDoS administrations or face lawful repercussions.

5. Conclusion

In conclusion, DDoS is a very serious type of attack, dealing with a DDoS mitigation is definitely a challenge. There are a lot of ways to use to destroy online services. A number of tools and generators explained in this paper and compared their workings. Many other tools and traffic generators also used in Cyberworld but I just analyzed some of them. This comparison surely helps experimenters to pick an appropriate tool or traffic

generators for their real experiments. Attackers update their attacks continuously like hit and run techniques. To avoid these attacks companies expend a lot of money, to mitigate and prevent this attacks now the law is in action against this cybercrime and a European Law enforcement organization closed a site who sold these tools.

References

[1] R., Xu, R., Tang, X., Sheng, V. S., & Cai, C. Cheng, "An abnormal network flow feature sequence prediction approach for DDoS attacks detection in the big data environment," 2018.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer (Long. Beach. Calif). vol. 50, no. 7, pp. 80–84, 2017.

[3] C., Miu, T. T., Luo, X., & Wang, J Wang, "Skyshield: A sketch-based defense system against application-layer DDoS attacks," 2018.

[4] V. Bukac, Traffic Characteristics of Common DoS Tools, Technical Report FIMU-RS-2014-02, 2014.

[5] 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.

[6] S. Behal and K. Kumar, "Characterization and comparison of DDoS attack tools and traffic generators - a review," Int. J. Netw. Secur., vol. 19, no. 3, pp. 383–393, 2017.

[7] T. Penttinen, "Distributed Denial-of-Service Attacks on the Internet," p. 148, 2005.

[8] A. Botta, A. Dainotti, and A. Pescape, "A tool for the generation of realistic network workload for emerging networking scenarios," Elsevier Journal of Computer Networks, vol. 56, no. 15, pp. 3531 {3547,2012}.

[9] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," Int. J. Comput. Appl., vol. 49, no. 7, pp. 24–32, 2012.

[10] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," International Jour- nal of Network and Computer Applications, vol. 40, pp. 307-324, 2014.

[11] Y. Huang, J. M Pullen, "Countering Denial-of-Service attacks Using Congestion Triggered Packet Sampling and Filtering", Proc. 10 th ICCCN, Oct. 2011.

[12] B. Sieklik, R. MacFarlane, and W. J. Buchanan, "Evaluation of TFTP DDoS amplification attack," Comput. Secur., vol. 57, no. November 2017, pp. 67–92, 2016.

[13] P. Wette and H. Karl, "DCT^{2}Gen: A Versatile TCP Traffic Generator for Data Centers," no. 4, pp. 1–15, 2014.

[14] S. Molnar, P. Megyesi, and G. Szabo, "How to validate traffic generators?," 2013 IEEE Int. Conf. Commun. Work. ICC 2013, no. October 2014, pp. 1340–1344, 2013

[15] Sourceforge, DDoS Attack Tools, (http://sourceforge.net/projects)

[16] S. M. S. M. K. K. Kumar S., "Flooding Based {DDoS} Attacks and Their Influence on Web Services," {IJCSIT} Int. J. Comput. Sci. Inf. Technol., vol. 2, no. 3, pp. 1131–1136, 2011.

Qaiser Abbas Khan is currently pursuing an MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: sp15mcs024@vcomsats.edu.pk

Usman Ali is currently pursuing an MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: r.usmaanali@gmail.com

Muhammad Kashif Nazir is a lecturer of computer science at RIPHAH International University, Pakistan, E-mail: kashif@riphahfsd.edu.pk

Rao Sohail Iqbal is a lecturer of computer science at GC University Faisalabad Pakistan, E-mail: raosohailiqbal@gcuf.edu.pk

Hina Zafar is currently pursuing an MS degree program in Computer Science at RIPHAH International University, Pakistan, E-mail: hinazfarsheikh@hotmail.com