Performance Comparison and Analysis of Slowloris, GoldenEye and Xerxes DDoS Attack Tools

Tanishka Shorey*, Deepthi Subbaiah, Ashwin Goyal, Anuraag Sakxena
School of Computer Science and Engineering
Vellore Institute of Technology, Vellore
Email: *tanishka1005@gmail.com

Alekha Kumar Mishra
Department of Computer Applications
National Institute of Technology Jamshedpur
Jamshedpur

***Abstract*—DDoS attack has been the most preferred attack by the hackers in the recent years. This is due to its ability to create multitude and variety of problems. A large group of hackers and experts in this field have developed packages and tools that initiate DDoS attack on various type of networks. It is essential to evaluate and compare the strength of DDoS attack launched by these tools to devise efficient countermeasures against it. In this paper, the performance of three DDoS attack tools is compared and analyzed using parameters such as time to successfully launch attack, traffic rate, and packet size. The DDoS tools considered for evaluation are Slowloris, GoldenEye and Xerxes. The experimental results infer that Xerxes outperforms other tools in launching a DDoS attack.**

***Index Terms*—DDoS, Attacker Tools, Performance Evaluation, Slowloris, GoldenEye, Xerxes.**

I. Introduction

The Denial-of-service (DoS) is a type of attack in which the hackers attempt to ward off genuine users from salvaging any service that is provided by either flooding or crashing them [1], [2]. A higher number of unsolicited messages probing the server/network are propelled by the hacker to authorize requests whose return addresses are unacceptable. Depending on the number of connections used, the DoS attack can be either a single-point attack or multi-point attack [3]. A single-point DoS attack normally makes use of a computer and only one Internet connection to overflow targeted system resources, whereas a multi-point Distributed DoS (DDoS) attack attempts to utilize an ample number of distributed computers as well as Internet connections to overflow a source making it a severe large-scale attack. Denial of Service(DoS) attacks affect organizations connected to the Internet by disrupting their business operations like e-commerce, banking, transportation etc. Over the last few years, the DDoS attacks have expanded in quality, sophistication, as well as the frequency at which they occur. In 2018, the biggest DDoS attack was launched on Github which flooded the Internet traffic at the rate of 1.35 terabits per second as reported by Fox News. The second largest attack was launched in 2016 by a Mirai botnet (an army of infected computers) on a cloud provider in France with 1.1 terabits per second. It is clear from the above attack incidents that DDoS has became a wide spread form of cyberthreat [4], [5]. Therefore, it is essential to study and analyze the behavior of this attack using the tools that are commonly used for this purpose.

The target of DDoS attacks is to scoff resources such as Cache, Main memory, CPU processing time, and bandwidth of a network connection. It makes these resources inaccessible to end users by either blocking network communication or denying access to these services [6]. Various tools are used malevolently by hackers to launch DDoS attacks although these tools were initially developed for testing the stress on a network [7]. In this paper, three DDoS tools are compared and evaluated to study the performance in terms of various attack parameters. The tools considered for comparison are Slowloris, GoldenEye, and Xerxes. The performance of the tools are compared in terms of time to successfully launch the attack, the traffic rate used, and average message size. This comparison aims to aid the researchers to choose the relevant DDoS attack tool traffic generator for effectively designing DDoS guard techniques.

Rest of the paper is organized in the following way. Section II provides a summary of defense mechanisms against DDoS in the recent years as reported in the literature. Section III gives an introduction to the attacker tools and classifies the attackers based on their characteristics. Section IV describes the attacking process in details by these tools and compare the experimental results followed by conclusions in Section VI.

II. Related Works

The Internet requires immediate attention and efficient countermeasures for DDoS attack due to its level of the threats on large networks. These methods must be flexible to be implemented at any level and depth of the network. Many attempts have been made to consolidate the information derived from various DDoS/DOS attack tools [8]. In the work proposed by Jelena and Peter [9], the attack characterization criteria was chosen to feature shared characteristics and essential highlights of the attack scheme. It is also used to define difficulties and direct the layout of countermeasures. The defense nomenclature classifies the form of the present DDoS defenses based on their design decisions. The work shows how these results edict the benefits and inadequacies of proposed arrangements. Feinstein *et al.* [10] have presented methods to detects the existence of DDoS attacks by comparing the entropy and frequency-sorted distributions of selected packet attributes. It is reported that DDoS attacks demonstrate aberrations in the features of the selected packet attributes. Evaluation of the per-

978-1-5386-5314-2/18/$31.00 ©2018 IEEE

formance in terms of detection efficiency is done by utilizing movement trace from a variety of network environments going from specific points in the core of the Internet to those inside edge networks. The results show that these techniques can be adequate against prevailing attacks and advise guidelines for enhancing detection of more surreptitious attacks. Li *et al.* [11] reported that the spike in the traffic rate and energy distribution using wavelet analysis can also be used to detect DDoS attack. A cluster analysis method is used for combative detection of DDoS by analyzing its attack plan hierarchy that comprises the attack type, selection of handler, agents, communication and compromised process [12]. Kulkarni and Bush [13] have proposed a distributed active network-based algorithm that utilizes attacker properties to correlate arbitrary traffic flows in the network to detect DDoS attacks. This algorithm has the advantage of not using any special filtering rules and hence suitable to detect any generic class of DDoS attack. Marciel *et al.* [14] have proposed a hierarchical model to represent the behavior of system components under DDoS attack. The model evaluate the attack feasibility, benefit and probability on these components. The attack tree can depict the severity of simultaneous attacks on the target system availability. Nagy *et al.* [15] have proposed a high-speed DDoS attack detector using FPGA. It is claimed that the detector can detect topmost DDoS attack types and most of the hit and run attacks within milliseconds.

The DDoS defense mechanisms as reported above are based on the behavior and characteristics of the attacker. Therefore, study and analysis of the attacker patterns and processes will provide a significant contribution towards effectively devising the defense mechanism. This paper aims to provide a comparative analysis of traffic pattern generated by recent and popular DDoS attacker tools.

III. DDoS Attacker Tools and Their Classification

In this section, we put forth the nature of DDoS attacking tools and their classification. Slowloris [16] is an effective tool that works by opening numerous connections to the directed web server and holding them open for indefinite period of time. Using these connections it transfers fractional HTTP requests unremittingly. As a result, the servers under attack keeps the connections open, while waiting for those fractional attack requests to be completed. A newer application compared to Slowloris is the GoldenEye [17], [18]. It is a python application for security testing purposes only. When used for malicious purpose, it has capable of bringing down its victim's web servers. The Xerxes, developed in 2017 is one of the most recent and powerful DDOS tools [19], [20]. It is developed using C and therefore requires a compilation phase. It uses port number 80 to attack on the web, resulting in blockage of responses from the web as the connection between the server and client ceases to exist. Remaining of the section provides the classification of attacker tools based on various characteristics.

A. Interface

The interface of a DDoS attacker tool can either be based on classical command line interpreter (CLI) or a graphical user interface (GUI). GoldenEye uses CLI, whereas XOIC tools uses GUI.

B. Attack Rate Dynamics

If the packets are sent continuously at a constant rate by the attacker, it is easily detected by the victim. Therefore, variable rate is used because these are more cautious while sending the packets. The rate dynamics may either increase uniformly or exists with variable fluctuations.

C. Attack category or vulnerability base

There are two types of DDoS based on attack target type: i) Attack on bandwidth depletion, and ii) Attack on resource depletion. In the bandwidth depletion type, the attacker floods the IP address by sending large number volumes of traffic. The target system either works very slow, crashes, or in the state of overloaded network bandwidth and prohibits the availability to legitimate users. The TCP SYN and PUSH+ACK are examples of these attacks. In the resource depletion type, malicious packets are sent to disrupt and misuse network protocol communications. As a result, the network resources are blocked and distorted.

D. Attack model architecture

Broadly there are two model architectures for DDoS: agent handler model, and reflector model. In the agent handler model, handlers are software packages placed throughout the Internet and are used by the attacker to launch the attack. Attacker periodically gains information about currently active and running agents. They aim at disrupting agent communication and load balancing. In the reflector model, the handlers have control over the agent. Hence, the attacker spoofs the IP address of the handler and manhandles the agent by flooding the victims IP address with packets. In IRC based model, a public Internet relay communication channel is established between the client and the agent for launching attacks.

E. Protocol

Flooding attacks are the major type of this category. Flood attacks are used to send a stream of SYN requests to clog and exhaust the victim network. This results in the network being unresponsive to legitimate users. One can have many types of flood attacks such as HTTP flood, TCP flood, UDP flood and ICMP flood.

F. Target area

In a network, an attacker can launch an attack either on links or endpoints. Endpoints usually mean the victims server so the attack is launched either on the server or the victim network as a whole.

IV. Proposed Work

The proposed work aims at implementing DoS attack on a common website, www.Chopy.krd using Slowloris, GoldenEye, and Xerxes. First, a study on the nature of network flow in each of the cases is done using a graphical network monitor application called Etherape. It shows the activities in link layer, IP and TCP modes. It uses GUI to display network activities. Host and link size is dynamic and changes with respect to current traffic. The color coded protocols helps to display the various protocol such as Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus several encapsulation formats. Etherape also supports traffic filtering either from live data or from stored traffic records. The website up/down status is verified on www.isitdownornot.com.

The source code of all the attacker tools are modified to incorporate a timer function in order to evaluate and juxtapose the activity execution duration.

A. Attack using Slowloris

The brainchild behind the well-crafted DDoS attack software, Slowloris is, Robert "RSnake" Hansen. The simplicity of this software is that only one computer is required to take down a web server. Adding to it's elegant nature, it does not affect other ports and services and solely affects the target. This tool requires no or low bandwidth to launch an attack. The name comes from the quality of the tool to 'slowly' consume the HTTP resources of the server. It is a HTTP DDoS attack tool and not to be confused as a TCP DDoS attack tool. This essentially means that, the tool makes a legitimate TCP connection with the target host and then floods the same with partial HTTP connections. These partial HTTP connections are kept open as long as possible and are continuously being sent so that all the resources of the target get exhausted. It's a smart move wherein the attacker is not sending malformed packets so these partial packets can easily slip through an intrusion prevention system.

The disadvantage of Slowloris is that the web servers of current generation have adequate resources to mitigate a Slowloris attack. These technologies includes

1) Expanding the highest number of customers that the web server will permit
2) Restraining the number of connections, a sole IP address is permitted to make
3) Restrictive conditions on the least possible transfer speed a connection are sanctioned to have
4) Inhibiting the time for each customer is permitted to remain linked

In Slowloris, a timer was implemented in between the source code of building sockets. This helps to compute the time taken to successfully build one socket. In an ideal condition, one socket is enough to bring down a website. Hence, the mean of the differences in time provides the time to bring down a website.

B. Attack using GoldenEye

GoldenEye is a HTTP/S Layer 7 DoS testing tool. KeepAlive (and Connection: keep-alive) paired with Cache-Control options is utilized to persevere the socket connection smashing via caching until it consumes all available sockets on the HTTP/S server. GoldenEye is an adroit and highly recommended tool which can successfully investigate the malware-focused environment. It can pro-actively capture malware's condition delicate quirks in cutting edge running, and choose the malware's likely focused on settings. It can also switch online its framework condition adaptively for promoting examination. GoldenEye can effectively figure out what is the malware's aimed environment via a particular conjectural execution engine to watch malware practices under elective situations.

GoldenEye, as it progresses adaptively, switches the environment, analyzes, and lets the malware itself reveal its objective, target, and environment. In spite of the fact that GoldenEye compromises space for speed, it has been seen that it could really utilize less memory space while accomplishing significantly higher speed. GoldenEye has been developed using python. The timer function is implemented in GoldenEye in such a way that the source code is independent of operating system environment.

C. Attack using Xerxes

It is one of the most recently developed DDoS attack tool by the hacker, 'The Jester' in 2017. This attack is not a traditional DDoS attack that uses several servers. It utilizes and exploits Apache HTTP by sending malformed packets that Apache HTTP takes several seconds to process, but only take a fraction of a second to send. By sending a few hundred of these per second it can keel over the Apache. This attack works by overwhelming the web server, rather than clogging the pipes to the server. As a result, the amount of bandwidth a server has is totally irrelevant. If a new server is added, then it just increases the traffic by n+1 to bring it down.

Table I summarizes and compare the common characteristics of the Slowloris, GoldenEye, and Xerxes tools. The compared parameters are the nature of the target, OS supported, the interface it uses and whether it provides IP Spoofing.

V. Experiments and Results

Table II, III, and IV shows the traffic characteristics of DDoS attack using Slowloris, GoldenEye, and Xerxes respectively at a particular instance of time. EtherApe was used to gather these information such as the instantaneous traffic, accumulated traffic, message size and port number. The major traffic is generated by Slowloris using HTTP and DNS since HTTP uses DNS for address resolution. However, GoldenEye and Xerxes mostly used HTTP traffic. Despite of lower traffic the accumulated traffic of HTTPS protocol is marginally below HTTP and DNS due to larger message payload. The attack traffic rate is higher in Slowloris and lower in GoldenEye. Table V shows the time required to successfully launch the DDoS attack by the above tools. It is observed that despite

TABLE I
COMPARISON OF COMMON CHARACTERISTICS.

Tool	Year	Implementation	Target		OS			Interface		IP Spoofing
			Bandwidth	Resource	Windows	Linux	MAC	CLI	GUI	
Slowloris	2009	Perl	✓	✓	✓	✓	-	✓	✓	No
GoldenEye	2012	Python	-	✓	✓	✓	✓	✓	-	No
Xerxes	2017	C	✓	✓	✓	✓	-	✓	-	No

of medium traffic, Xerxes is bring down the target in 0.038 milliseconds which is significantly powerful and far from the performance of Slowloris and GoldenEye. This is due to its intelligent and adaptive traffic rate that helps to achieve this time. The Figure 1 provides a snapshot of initial network status before attack. The Figure 2, 3, and 4 shows snapshots of attack traffic of Slowloris, GoldenEye, and Xerxes using EtherApe respectively. Here, blue color circle indicates heavy DNS traffic, and red colored circles indicate heavy HTTP traffic.

TABLE II
SNAPSHOT OF ATTACK CHARACTERISTICS OF SLOWLORIS.

Protocol	Instantaneous Traffic Rate	Accumulated Traffic	Message size (Bytes)	Port
DNS	719.83Kbps	6.08 Mb	142 bytes	53
HTTP	746.58Kbps	7.15 Mb	119 bytes	80
HTTPS	1.50Kbps	3.47Mb	751 bytes	443
ICMPV6	0bps	2.24Kb	88 bytes	-
IGMP	0bps	378 bytes	54 bytes	-
MDNS	0bps	3.16Kbytes	154 bytes	5353
NETBIOS-NS	0bps	552 bytes	92 bytes	137
NTP	0bps	660 bytes	110 bytes	123

TABLE III
SNAPSHOT OF ATTACK CHARACTERISTICS OF GOLDENEYE.

Protocol	Instantaneous Traffic Rate	Accumulated Traffic	Message size (Bytes)	Port
DNS	7.00Kbps	376.60 Kb	139 bytes	53
FRAGMENT	0bps	762 bytes	95 bytes	-
HTTP	98.39Kbps	1.29 Mb	220 bytes	80
HTTPS	2.10Kbps	229.50 Kb	493 bytes	443
ICMPV6	0bps	1.44 Kb	82 bytes	-
MDNS	0bps	874 bytes	146 bytes	5353
NTP	0bps	220 bytes	110 bytes	123
TCP -UNKNOWN	0bps	1.32 Kbytes	338 bytes	-

VI. CONCLUSION

In this paper, three DDoS attack tools are studied and analyzed with respect to their attack characteristics. These tools are Slowloris, GoldenEye, and Xerxes. All the tools mostly use

TABLE IV
SNAPSHOT OF ATTACK CHARACTERISTICS OF XERXES.

Protocol	Instantaneous Traffic Rate	Accumulated Traffic	Message size (Bytes)	Port
DNS	6.41Kbps	614.14 Kb	138 bytes	53
FRAGMENT	0bps	762 bytes	95 bytes	-
HTTP	560.97Kbps	4.85 Mb	113 bytes	80
HTTPS	0bps	240.38 Kb	435 bytes	443
ICMPV6	0bps	2.72 Kb	82 bytes	-
MDNS	0bps	1.04 Kbytes	134 bytes	5353
NTP	0bps	220 bytes	110 bytes	123
TCP -UNKNOWN	0bps	1.32 Kbytes	338 bytes	-

TABLE V
DDOS ATTACK RESULTS.

Tool	Attack Traffic	Accumulated Traffic level	Mean Attack Time (ms)
Slowloris	http	High	100.0
GoldenEye	http	Low	6.216526
Xerxes	http	Medium	0.038

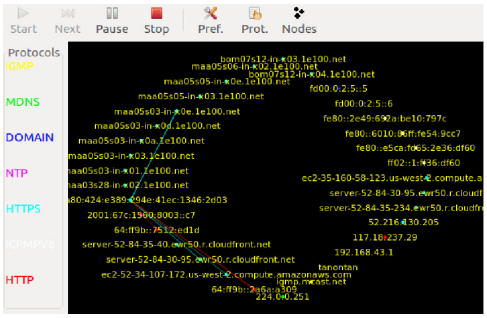

Fig. 1. Initial status of the network.

HTTP traffic to launch DDoS attack. Slowloris is a kind of naive tool, whereas GoldenEye and Xerxes uses sophisticated logic to launch the attack. The accumulated traffic of Slowloris is higher compared to others. The attack results shows that Xerxes has outperformed GoldenEye and Slowloris in terms of time required to successfully launch the DDoS attack. This contribution aims to provides a characteristics of these tools in order to devise effective countermeasures against DDoS.

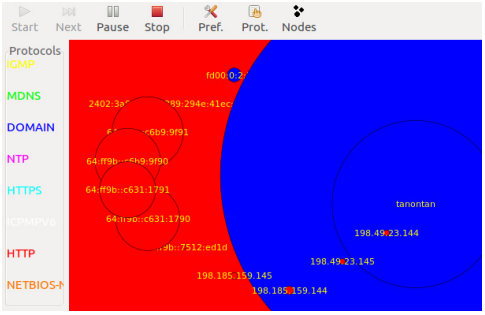

Fig. 2. Network status after attack by Slowloris.

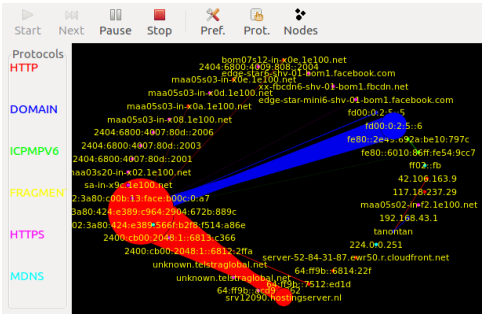

Fig. 3. Network status after attack by GoldenEye.

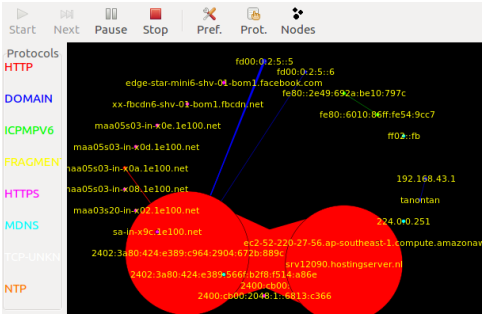

Fig. 4. Network status after attack by Xerxes.

REFERENCES

[1] J. Smith-perrone and J. Sims, "Securing cloud, sdn and large data network environments from emerging ddos attacks," in *2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence*, Jan 2017, pp. 466–469.

[2] K. Alieyan, M. M. Kadhum, M. Anbar, S. U. Rehman, and N. K. A. Alajmi, "An overview of ddos attacks based on dns," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2016, pp. 276–280.

[3] B.B.Gupta, R. C. Joshi, and M. Misra, "Defending against distributed denial of service attacks: Issues and challenges," *Information Security Journal: A Global Perspective*, vol. 18, no. 5, pp. 224–247, 2009.

[4] S. Kumar and K. M. Carley, "Ddos cyber-attacks network: Whos attacking whom."

[5] Y. Xie and S.-Z. Yu, "Monitoring the application-layer ddos attacks for popular websites," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 15–25, February 2009.

[6] D. Yin, L. Zhang, and K. Yang, "A ddos attack detection and mitigation with software-defined internet of things framework," *IEEE Access*, pp. 1–1, 2018.

[7] J. Choi, C. Choi, B. Ko, and P. Kim, "A method of ddos attack detection using http packet pattern and rule engine in cloud computing environment," *Soft Computing*, vol. 18, no. 9, pp. 1697–1703, September 2014.

[8] R. Latif, H. Abbas, and S. Assar, "Distributed denial of service (ddos) attack in cloud- assisted wireless body area networks: A systematic literature review," vol. 128, no. 38, November 2014.

[9] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, April 2004.

[10] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to ddos attack detection and response," in *Proceedings DARPA Information Survivability Conference and Exposition*, vol. 1, April 2003, pp. 303–314 vol.1.

[11] L. Li and G. Lee, "Ddos attack detection and wavelets," in *Proceedings. 12th International Conference on Computer Communications and Networks (IEEE Cat. No.03EX712)*, Oct 2003, pp. 421–427.

[12] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "Ddos attack detection method using cluster analysis," *Expert Systems with Applications*, vol. 34, no. 3, pp. 1659–1665, 2008.

[13] A. Kulkarni and S. Bush, "Detecting distributed denial-of-service attacks using kolmogorov complexity metrics," *Journal of Network and Systems Management*, vol. 14, no. 1, pp. 69–80, March 2006.

[14] R. Maciel, J. Araujo, J. Dantas, C. Melo, E. Guedes, and P. Maciel, "Impact of a ddos attack on computer systems: An approach based on an attack tree model," in *2018 Annual IEEE International Systems Conference (SysCon)*, April 2018, pp. 1–8.

[15] B. Nagy, P. Orosz, T. Tthfalusi, L. Kovcs, and P. Varga, "Detecting ddos attacks within milliseconds by using fpga-based hardware acceleration," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, April 2018, pp. 1–4.

[16] V. Bukac and V. Matyas, "Analyzing traffic features of common standalone dos attack tools," in *International Conference on Security, Privacy, and Applied Cryptography Engineering*, October 2015, pp. 21–40.

[17] S. Gurubaran, "Ddos a website anonymously by using kali linux tools." [Online]. Available: https://gbhackers.com/anonymous-ddos-a-website-using-kali-linux/

[18] "Goldeneye." [Online]. Available: https://github.com/jseidl/GoldenEye

[19] S. Gurubaran, "Xerxes most powerful tool for dos attack using kali linux." [Online]. Available: https://gbhackers.com/xerxes-kali-linux-tutorial/

[20] "Xerxes." [Online]. Available: https://github.com/zanyarjamal/xerxes