TEST Engineering & Management

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

Mitigation of TCP and UDP Based Distributed Denial of Service Attacks

RasheedaIdrisAbdulkadir, Dr. Muhammad Aminu Ahmed, Umar FarukAbdulhamid, Abdullahi Umar Diso
[1]Department of Computer Science
Kaduna State University, Kaduna, Nigeria.
rasheeda.abdulkadir@kasu.edu.ng, sahalu@abu.edu.ng, umar.abdulhamid@kasu.edu.ng, abduldiso@kasu.edu.ng,

Article Info
Volume 82
Page Number: 12225 - 12232
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 23 February 2020*

Abstract
Denial of Service (DoS) attacks are serious threats to information availability as they deny users access to computer network or system, which can be very damaging to organizations. Although DoSattacks cannot be completely stopped, various defense mechanisms have been proposed and implemented. These mechanisms are anomaly-based detection techniques that use the concept of a baseline for network behavior. Any deviation from this established baseline is considered as an anomaly. These solutions are usually deployed on routers to protect internal computer network because detection at the victim end is easily achieved. However, most of these solutions only detect attacks, while administrators usually deploy the response and countermeasure manually. Detection alone may be useful in alerting human administrators for the presence of an attack and notifying upstream (closer to attack sources) devices, but unable to stop the attack automatically. For Distributed Denial of Service (DDOS) attacks, lack of an automated solution to mitigate the attack can cause serious consequences due to the high frequency and volume of traffic generated from malicious attackers against the target before manual countermeasures are applied. This research work presents a system that uses behavioral signatures to detect and mitigate DDOS attacks. It also compares the proposed system to an off-the-shelf solution (SNORT) in order to assess efficiency.

Keywords:*DDOS, Detection, Mitigation*

I. INTRODUCTION

Most organizations today, irrespective of size or distribution, use computer systems and networks to share information locally, and use Internet services such as sending and receiving mails, share business related information with partners, process customer requests and information, advertisements and other services. As a result, the confidentiality and availability of data held and processed by server hosts and other network infrastructure must be maintained and protected from unauthorized access and disruption.

Denial of service (DoS) implies that an attacker disables or corrupts computer networks, systems or services with the intent to deny access to these Resources by intended users[1]. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable [1]. However, DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are one of the biggest concerns for security professionals [2]. Distributed Denial of Service attack is the use of many-compromisedsystems working towards making information and data unavailable to a single target.

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

Several anomaly detection systems have been developed to identifyDDoS attacks. However, they use complex algorithms or methods to distinguish between benign and attack traffic. This adds to the computation time of the system making it lag for a few seconds before detecting attacks. Also, these systems only detect DDoS attacks and set off an alarm to alert the network administrator. Thus, they do not mitigate an identified attack. Mitigation is important because DDoS attacks can cripple a server/network in the few minutes needed for the system administrator to tackle the situation.

This paper presents a network level solution that identifiesDDoS attacks using minimal set of traffic features (by analyzing TCP/IP and UDP packet header) that characterize DDoS attacks in order to reduce the complexity of the detection process. The solution also automatically mitigates the identified DDoS intrusion by dropping/suspending inbound DDoSpackets and datagrams. This ensures that network system and services are not cripple by the DDoS attack in a short period while providing network administrators with enough time to resolve the situation. The research also compares the proposed solution against an existing solution (SNORT) to assess the effectiveness of the proposed solution.

The remaining part of the article is organized as follows; Section 2 present a survey of related work on DoS detection and response mechanisms. Section 3 discusses the proposed DDoS detection and mitigation solution. Section 4 discusses the evaluation procedure used to test both the solution proposed and the existing solution (SNORT). Section 5 presents and discusses the results of the evaluation, while Section 6 concludes the paper and suggest future work.

II. RELATED WORK

The mechanisms used to detect and counter DDoS attacks can be categorized as detection, prevention, response and tolerance [3]. Detection is used to monitor a network or system's traffic to identify malicious packets or datagram that may cause denial of attack. Prevention is used to stop DDoS attacks from occurring. Response occurs after an attack or detection of an attack. It eliminates or reduces the impact of the attack. Tolerance is used to reduce the damage caused by a DDoS attack without differentiating between malicious and legitimate traffic. It focuses on maximizing quality of service during an attack. The review focuses on schemes that use detection and response mechanisms.

2.1 Detection Mechanisms

The detection mechanisms used to identify network intrusions are classified as signature and anomaly-based detection systems.

[4] proposed a DoS detection method for all the attack scenarios given by [5] which are; constant rate, pulsing rate, increasing rate and sub-group. A statistical approach was used to detect any abnormalities or change in traffic flow. When any abnormality is detected, an alarm is generated.

[6]proposed an abnormal network flow feature sequence prediction approach which could be used as a DDoS attack detector in the big data environment. They defined a network flow abnormal index as PDRA with the percentage of old IP addresses, the increment of the new IP addresses, the ratio of new IP addresses to the old IP addresses and average accessing rate of each new IP address. An IP address database was designed using sequential storage model which has a constant time complexity. The autoregressive integrated moving average (ARIMA) trending prediction module will be started if and only if the number of continuous PDRA sequence value, which all exceed an PDRA abnormal threshold (PAT), reaches a certain preset threshold. And then calculate the probability that is the percentage of forecasting PDRA sequence value which exceed the PAT. DDoS attack was identified based on the abnormal probability of the forecasting PDRA sequence.

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

The reported DoS detection mechanisms used abnormal behaviour to identify attack traffic and generate an alert. The limitation of this type of system is that it requires human intervention to prevent the attack because it lacks an automatic mitigation solution. An administrator would have to be on site in order to assess the threat and direct the system on what to do.

Response Mechanisms

Response mechanisms are usually initiated after the detection of an attack to eliminate or minimize the impact of the attack.

[7] proposed Reinforcing Anti-DDoS Actions in Realtime (RADAR) to detect and throttle DDoS attacks via adaptive correlation analysis built upon unmodified commercial off-the-shelf SDN switches. The system defends against a wide range of flooding-based DDoS attacks, e.g., link flooding (including Crossfire), SYN flooding, and UDP-based amplification attacks, while requiring neither modifications in SDN switches/protocols nor extra appliances. It accurately detects attacks by identifying attack features in suspicious flows, and locates attackers (or victims) to throttle the attack traffic by adaptive correlation analysis.[8]also proposed an application calledVFence - a defense mechanism against DDoS attack that leverages the capability of the Network Function Virtualization (NFV) architecture. NFV is the technology of virtualizing network functions in virtual machines on commodity servers and it allows a flexible and dynamic implementation of the network functions. The proposed mechanism uses network agents to intercept packets when the system is potentially under attack, to verify their authenticity, and to keep the server safe by dropping illegitimate packets. Since the attack intensity often varies,the NFV-based defense framework deploys agents dynamically to balance the attack load

Research Gap

Anomaly detection systems developed so far for detecting DDoS attacks use complex algorithms or methods to distinguish between benign and attack traffic, this adds to the computation time of the system making it lag for a few seconds before detecting attacks. Also, some of these systems only detect DDOS attacks and set off an alarm to alert the network administrator, the systems do not to stop or mitigate the attack. DDoS attacks can cripple a server/network in the few minutes needed for the system administrator to tackle the situation.

III. The DDoS Mitigation Approach

TCP is a connection-oriented protocol. It uses various flags to indicate that a connection is being started or ended, or that the data carries a high priority[9]Many attacks are based on altering the TCP flags. Certain illegal combinations of TCP flags may be able to help packets avoid detection by firewalls or intrusion detection systems; other illegal combinations may be used to attack the systems[9]. Below are the various flags in a TCP protocol:

1. SYN (Synchronization): This flag is used to initiate a TCP connection.
2. ACK (Acknowledgment): This flag is used to indicate acknowledgment.
3. FIN (Finish): This flag is used to gracefully end a TCP connection.
4. RST (Reset): This flag is used to immediately end a TCP connection.
5. PSH (Push): This flag is used to tell a receiver to pass on the data as soon as possible.
6. URG (Urgent): This flag is used to indicate that the urgent pointer is valid.

There are certain combinations of flags that are accepted and are legal [10]. These are:

1. SYN, SYN ACK, and ACK are used during the three-way handshake, which establishes a TCP connection.

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

2. Every packet in a connection must have the ACK bit set, except the initialization packet, i.e., the initial SYN packet.
3. FIN ACK and ACK are used during the graceful teardown of an existing connection.
4. PSH FIN ACK may also be seen at the beginning of a graceful teardown.
5. RST or RST ACK can be used to immediately terminate an existing connection. Packets during the "conversation" portion of the connection (after the three-way handshake but before the teardown or termination) contain just an ACK by default. Optionally, they may also contain PSH and/or URG.

The combinations of flags that are abnormal are[11]:

1. SYN and FIN is an illegal combination because SYN is used to start a connection while FIN is used to end an existing connection. Thus, it is illegal to perform both actions at the same time. Scanning tools also use this combination.
2. SYN FIN PSH, SYN FIN RST, and SYN FIN RST PSH - These packets may be used by attackers and are clearly malicious.
3. Packets should never contain just a FIN flag. FIN packets are frequently used for port scans, network mapping and other stealth activities.
4. It is illegal to have a packet with no flags set.
5. It is abnormal to have either or both TCP reserved bit turn on.
6. Packets should never have a source or destination port set to 0.
7. The acknowledgment number should never be set to 0 when the ACK flag is set.
8. A SYN only packet, which should only occur when a new connection is being initiated, should not contain any data.
9. Destination address of a packet should not be to a broadcast

TCP-based attacks also involve sending multiple copies of SYN packets to a target within few seconds in order to keep the target waiting for ACK/SYN packet. This is known as SYN flooding.Abnormalities concerning UDP datagrams are detected when a client sends identical multiple datagram requests to a server in a few seconds. UDP datagrams should also never have a source or destination port set to zero.

The abnormal TCP flag combinations, TCP SYN and UDP flooding and abnormal UDP source and destination ports are used as behavioral signatures in theproposedDDoS attack mitigation system. Figure 3 presents the design of the DDoS detection and mitigation system. The system comprises Traffic classification and DDoS Detection and Mitigation components and activity logs as shown in Figure 1.

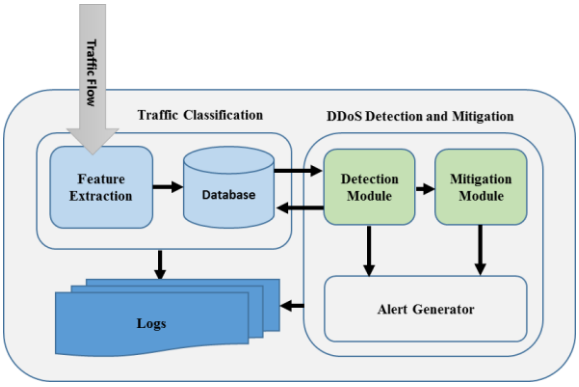

Figure 1: Architecture of the DDoS mitigation system

The Traffic Classification component inspects all inbound traffic and classifies the traffic based on the transmission protocols. The module uses the feature extraction module to filter TCP and UDP packets and keeps the record in a database for the DDoS detection module.

The DDoS Detection and Mitigation component determines anomalous TCP and UDP header information for DoS attack using the detection module. Upon exceeding a set limit for anomalous behavior by a remote host, the detection module then passes the IP address of the host to the mitigation module for suspension. The mitigation module applies network access control for packets that have been identified as DoS intrusions. Before an IP address is suspended, it should have

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

exceeded the threshold value assigned for by a network administrator based on the requirement of the network and traffic characteristics.

The detection and mitigation modules to raise an alarm when the system detects a DDoS attack and suspends an external IP address trigger the alert generator.

The Traffic Classification and DDoS detection and mitigations components keep record of network activities in the logs. The logs comprise files for traffic, DDoS detection and DDoS mitigation logs.

IV. EVALUATION

The proposed DDoS mitigation mechanism was implemented using python programming language. The evaluation uses a testbed a number of experiments to test the performance of the DDoS detection system.The detection capability of the system was assessed using the following set of metrics:

a. True Positive: This is the number of intrusions that are successfully detected and mitigated.
b. False Positive: This is the number of normal traffic that is wrongly classified as intrusions.
c. True Negative: This is the number of normal traffic that is successfully labeled as benign traffic.
d. False Negative: This is the number of intrusions that are missed and classified as normal traffic.

The performance of the mechanismwas then quantified using the following metrics [12]

1. False Positive Rate: ratio between the numbers ofnormal instances detected as attack and the total number of normal instances.

$$\frac{FP}{TN + FP} \quad (1)$$

2. True Positive Rate: ratio between the number of attack traffic that are classified as normal and the total number of attacks.

$$\frac{TN + FN}{TP + TN + FP + FN} \quad (2)$$

3. Accuracy – How often is the IDS correct? This can be calculated by

$$\frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

4. Precision – when it predicts yes, how often is it correct? This is calculated by

$$\frac{TP}{TP + FP} \quad (4)$$

4.1 Test Bed

The test bed used for the experimentation comprises a victim server with Windows Server 2012 operating system, five (5) computers for DDoS Attack generation, One computer for benign traffic generation, a router and anethernetswitch. The testbedis depicted in Figure 2.

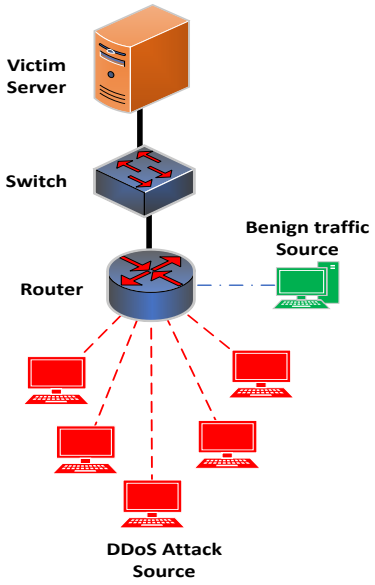

Figure 2: Layout of the evaluation testbed

The five (5) attacking computers have Windows 10 OS installed and were equipped with intel® Pentium, 2.41 GHz processor, 8GB of RAM, 1TB of hard disk space. Each computer simulated twenty (20) instances ofDDoS attacks with different IP addresses, making a total of one hundred (100) simulated computers that send DDoS attacks to the victim server. Ostinato [] was

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

installed on each of the five computers to enable DDoS attack generation. Ostinato is open-source software the crafts packets, generates and analyses any type of traffic [13]. It has a Graphical User Interface (GUI), which makes it easy to use. In this research it was used to craft and send attack packets.

The benign traffic-generating computer has Ubuntu operating system with Tcpreplay installed. Tcpreplay is an open source suite of utilities used for editing and replaying previously captured network traffic. It has tools that can classify traffic as client and server traffic and replays that traffic so it seems like the communication is occurring at that particular time. Tcpreplaywas used to generate background traffic using the MACCDC (Mid-Atlantic Collegiate Cyber Defense Competition) dataset. Tcpreplaywas used to replay benign traffic to the victim server in client server fashionthrough the gateway.

Therouter is a computer with Ubuntu operating system and Quagga routing suite installed and configured as a router. The proposed DDoS mitigation system was hosted on this computer.

Finally, the dataset used as benign traffic is the MACCDC 2014 dataset.The dataset comprises traffic from a cyber defense competition that incorporated a set of hosts used for network attack and another set of hosts for benign traffic generation. The recorded benign traffic was generated using 20 hosts by manually interacting with web, email, DNS lookups, and other required services. This research work uses the benign traffic of the MACCDC 2014 dataset.

Experimentation

The evaluation was conducted in three sets of experiments. Each set comprises three experiments using a number of attack and benign traffic sent per second with different threshold values as shown in Table 1

Table 1: Set of Experiments Conducted

#	Traffic (pps)		Threshold Values		
	Attack	Benign	2	5	10
1	500	50	✓	X	X
	500	50	X	✓	X
	500	50	X	X	✓
2	1000	100	✓	X	X
	1000	100	X	✓	X
	1000	100	X	X	✓
3	1500	100	✓	X	X
	1500	100	X	✓	X
	1500	100	X	X	✓

The sets of experiments were conducted without the DDoS detection system in place. The experiments were then repeated with the DDoS mitigation system installed in the router. Lastly, the same set of experiments were conducted with SNORT installed in the router.Eachof the nine experiments were repeated three times, and average result of the experiments was taken. The attack traffic consists of TCP packets with abnormal flags, SYN and UDP flooding and UDP packets with source and destination ports set to 0 in the ratio of 3:2 (60% TCP and 40% UDP).A total number of 27 experiments with the DDoS Mitigation system were conducted during the evaluation.

V. Discussion of Results

The results of the experiments conducted are discussed in this section.

An experiment was conducted with each of the five attacking computers sending500 attack traffic per second against the server without the DDoS Mitigation system in place. No significant change was observed on the transmission rate of traffic sent and received by the server. The experiment was repeated with1000 attack traffic per second, whichslowed down the server.Eventually, the server stopped responding to traffic requests. In the third experiment, the attack traffic was increased to 1500 packets per second respectively without the DDoS mitigation system. The server stopped responding to traffic and froze completely. The three experiments were conducted to establish a DDoS attack scenario

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

prior to deployment of the proposed DDoS mitigation system.

Table 2 shows the results of the experiments conducted with the DDoS Mitigation System and SNORT in place.

	DDOS Mitigation System					SNORT			
Ex.	Threshold	FPR	TPR	Precision	Accuracy	FPR	TPR	Precision	Accuracy
1	2	0.00	0.99	99%	99%	0.54	0.92	93%	60%
	5	0.00	0.94	99%	94%	0.39	0.71	90%	50%
	10	0.00	0.65	99%	67%	0.37	0.66	91%	30%
2	2	0.00	0.98	99%	99%	0.50	0.64	93%	60%
	5	0.00	0.73	99%	75%	0.56	0.51	90%	50%
	10	0.00	0.55	99%	50%	0.29	0.28	91%	30%
3	2	0.00	0.81	99%	83%	0.17	0.54	96%	54%
	5	0.00	0.69	99%	75%	0.13	0.37	96%	40%
	10	0.00	0.59	99%	64%	0.11	0.37	96%	40%

Table 2.TPR, FPR, Precision and Accuracy of the DDoS Mitigation System and SNORT in the three Sets of Experiments

The false positive rates of the DDoS mitigation system are zero in all the nine experiments. This is because the number of false positives observed during the experiments ranges from 11 to 35 out of more than a million packets. The results also showed that the true positive rate of the mitigation system reduces with increasing number of threshold value in all the three experiments, which is due to the increasing number of false negatives. This shows that increasing the number of allowedDDoStrafficbefore blocking the source increases the changes of classifying benign traffic as DDoS packets.

Furthermore, the precision of the DDoS mitigation system was 99% across the entire set of experiments. This is due to the few numbers of false positives raised by the DDoS mitigation system. Additionally, the accuracy of the DDoS mitigation system varies with increasing number of threshold value and volume of attack traffic. This is due to the increasing number of false negatives as the threshold value and attack traffic increase.

With SNORT, the false positive rates are higher. Rate filtering, which is used in Snort to detect DDoS attacks that are not in the signature database.

VI. CONCLUSION AND FUTURE WORK

This research presented a lightweight autonomous anomaly detection system that detects and mitigates denial of service attacks. It uses minimal set of traffic features found in a packet header to determine whether traffic is malicious or benign. When an attack is detected, it uses already installed IPtables in Ubuntu to rewrite firewall rules so the source of attack is blocked.The solution was compared with Snort, a lightweight, signature-based detection system, which has a rate-limiting feature to detect DDoS attacks that are not in the signature database. Further work can also be carried out on this solution to make it more efficient. To stop the solution from dropping packets at high traffic rates, multithreading could be employed so that the proposed solution can take advantage of multiple processors. The proposed software should also be able to detect spoofed IP addresses. The solution can be extended to detect and defend against low rate DDoS attacks. The solution could also be extended to work with IPv6 addresses.

VII. REFERENCES

[1] Alabady, S. A. J. Design and Implementation of a Network Security Model using Static VLAN and AAA Server. 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications.

[2] Zargar S. T., Joshi J., and Tipper D., A Survey of Defense Mechanisms Against Distributed Denial

January - February2020
ISSN: 0193-4120 Page No. 12225 - 12232

of Service (DDoS) Flooding Attacks. In IEEE COMMUNICATIONS SURVEYS & TUTORIALS.

[3] ABLIZ 2011 Internet Denial of Service Attacks and Defense Mechanisms.InUniversity of Pittsburgh Technical Report, No. TR-11-178, March 2011.

[4] Buragohain C., Bhattacharyya K., Kalita M., Singh S. Anomaly Based DDoS Attack Detection. In International Journal of Computer Applications (09-75-8887) volume 123 – No. 17. August 2015.

[5] Mirkovic, J., Prier, G., and Reiher, P. (2002) Attacking DDoS at the source. Proceedings of the 10thIEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS.

[6] Renjie Cheng, RuomengXu, Xiangyan Tang, Victor S Sheng, Canting Cai. An abnormal network flow feature sequence prediction approach for DDoSattacks detection in big data environment. https://doi.org/10.3970/cmc.2018.055.095. Vol 55 No 1 (2018)

[7] Jing Zheng; Qi Li; GuofeiG ;Jiahao Cao; David K. Y. Yau ; Jianping Wu. RealtimeDDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis. IEEE Transactions on Information Forensics and Security (Volume: 13, Issue: 7, July 2018)

[8] A H M Jakaria; Wei Yang; BahmanRashidi; Carol Fung; M. AshiqurRahman. VFence: A Defense against Distributed Denial of Service Attacks Using Network Function Virtualization 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).10.1109/COMPSAC.2016.219

[9] SaravananKumarasamy, A.Gowrishankar. An Active Defense Mechanism for TCP SYN flooding attacks.arXiv:1201.2103 [cs.CR] 2012.

[10] Bruneau,G.(2000).seeker_tcp_header.html. Retrieved from http://www.whitehats.ca: http://www.whitehats.ca/main/members/Seeker/seeker_tcp_header/seeker_tcp_header.html

[11] Antoniou, S. (2009, may 14). ping of death and dos attacks. Retrieved from www.pluralsight.com.

[12] Markham, k. (2014, march 25). simple-guide-to-confusion-matrix-terminology.Retrieved from http://webcache.googleusercontent.com:http://webcache.googleusercontent.com/search?q=cache:http://www.dataschool.io/simple-guide-to-confusion-matrix-terminology/communication Review 32, 62–73.

[13] osinato.org. (2017). Retrieved from osinato.org