Security methods of servers against attack

Shaila Ghanti , G.M.Naik
Department of Electronics, Goa University, Goa, India.

ABSTRACT: Information and technology devices are being used extensively these days on the internet. Distributed Denial of Service (DDoS) attacks generated on the server denies the access of the server to the genuine users. The servers needs to be protected from the DDoS attack. In this paper we compare the different defense mechanisms used to protect the DDoS attack. The defense mechanisms used must ensure better network resource utilization.

Keywords: *Attacks, Denial of service, Network Resource utilization*

I. INTRODUCTION

Evans [1] suggests that in future there will be huge amount of embedded systems and IOT devices will be used. As large amount of IT devices will be used in future the problems related to E-waste, wasting of electricity will be increased. There is a need to maximize the energy efficiency used by the IT devices over the life span of the device [2]. In these days DDoS attacks are being generated by malicious users on the internet. These attacks deny the server access to the genuine users and hence there is a need to defend these attacks. To defend the attack on the network, packets need to be analysed and action needs to be taken. The Power consumption of router increases as the traffic throughput increases [3]. The power consumption of resources and Network resource utilization are the important parameters to be considered while selecting the type of defense mechanisms to be used.

II. DDOS ATTACKS

DDoS attack is an attack generated by malicious users on the server so that the services of that server are not available to the genuine users. The main intentions of generating DDoS attacks are financial gain, to take revenge, to experiment with the attacks , just to show off the their talent. Servers were affected due to attack and huge amount of loss incurred due to these attacks [4]. DDoS attacks are generated from large amount of compromised computers called zombies on the victim only after getting the instructions from the attacker as shown in figure 1 . Here large amount of attack packets are generated from large number of compromised machine that generates attacks to the server. These attacks generated sends huge amount of packets that pass through the routers in the subnet to reach to the destination. These attack packets utilizes the resources of network like routers, firewall to reach to the victim. These large amounts of packets when pass through the routers the power consumption is also increased. Unnecessarily the power consumption is increased. Hence there is a need to protect the servers from these attacks so that power consumption must be minimum and network resources should be used efficiently.

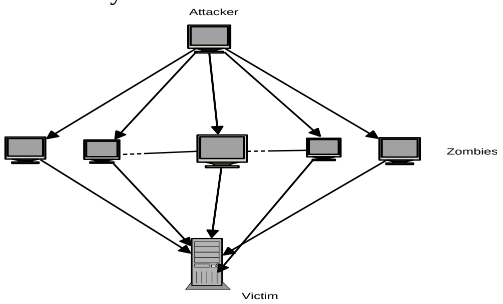


Figure 1 DDoS attack

The Experimental set up

We set up a network of three computers as shown in figure 2 and the server was configured as web server. The other machine was used as router by adding two network interface card. Another computer is used as client that generates the genuine attacks and genuine requests to the server.

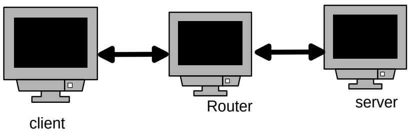
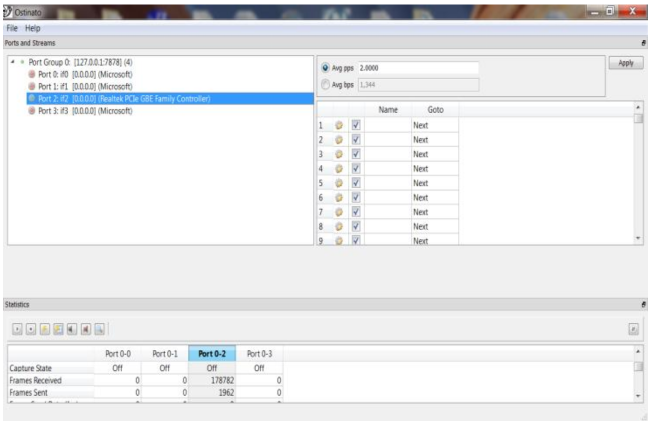


Figure 2. Experimental set up

Client sends huge amount of attack packets to the server as well as genuine clients. To generate attack packets ostinato tool [5] is used and ab tool [6] is used to generate genuine requests to the web server. Figure 3 shows the ostinato tool used to generate attack packets. On the server wireshark packet capture tool [7] was used to capture packets. It is observed that attack packets as well as genuine packets reach to the destination. The service provided by the server is blocked due to which genuine clients will not be able to access the web pages.



- Port Group 0: [127.0.0.1:7878] (4)
  - Port 0: if0 [0.0.0.0] (Microsoft)
  - Port 1: if1 [0.0.0.0] (Microsoft)
  - Port 2: if2 [0.0.0.0] (Realtek PCIe GBE Family Controller)
  - Port 3: if3 [0.0.0.0] (Microsoft)

● Avg pps 2.0000
○ Avg bps 1,344

			Name	Goto
1		☑		Next
2		☑		Next
3		☑		Next
4		☑		Next
5		☑		Next
6		☑		Next
7		☑		Next
8		☑		Next
9		☑		Next

	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Capture State	Off	Off	Off	Off
Frames Received	0	0	178782	0
Frames Sent	0	0	1962	0

Figure 3. Attacks generator

These attack packets generated by the client are all processed in the router and forwarded to the server. The attack packets uses the network resource like router and server. Unnecessarily these packets are processed by the router and server as a result there will be increase in power consumption also the access to the server is denied. Hence there is a need to defend these attacks .

III. DDOS DEFENSE METHODS

All the methods used to defend the DDoS attack methods are classified into three types depending on the location of deployment. They are victim side, intermediate routers side and source side defense mechanisms.

Victim side Protection:

There are many methods available [8, 9] that can protect the victim or server by employing these defense mechanisms at the victim side. The defense mechanisms are deployed at the victim side as a part of end router or server. Hop count filtering: Hop count filtering [8] is deployed at the victim side. In this method it maintains the table related to the source IP addresses and normal number of hops required to reach the destination when there is no attack. When the incoming packet source IP address and the number of hops used to reach the destination doesn't match with the hop filter table then those packets are filtered. It indicates that the incoming packet could be spoofed. Hence these are identified as the attack packets and are filtered by the defense mechanisms. SYN Cookie : This is common method of filtering deployed at the victim side to protect the victim from the attacks. In this method [9] when the SYN packet is received the usual state information that is maintained normally by the receiver are used and added that information as the sequence number of SYN-ACK. Hence the receiver need not maintain any state information. Discussion: Generally victim side protection methods are preferred as it has to be deployed at the respective victim side only. There is no need that it has to be deployed for all the victims. When victim side defense mechanisms are used the attack packets generated by the attacker travels all through the different routers between the source and the destination and the attacks are handled at the victim side only. Every incoming attack packet is received by the router, reads the related information from the packet and forwards these packets to the corresponding interface. As large amount of attack packets are generated by the zombies large amount of packet processing is done by the router. This increases the power consumption of routers and network resources are utilized in processing attack packets. Therefore the victim side defense mechanisms are not efficient as the network resources are not used properly.

IV. INTERMEDIATE ROUTER SIDE PROTECTION:

These defense mechanisms [10, 11]are deployed on the routers inside the network so that the servers can be protected from attack.Packet Marking : The routers needs to mark the packets [10] that are forwarded by the router that will help the to defend the attack packets.Detecting compromised router: the routers that are compromised are detected using this method [11].Discussion: In these methods the defense mechanisms are deployed on the routers in the network. In this case also the attack packets are forwarded through all the routers. Hence the network resources are utilised for processing large amount of attack packets. Similar to victim side defense mechanisms these methods are not efficient as the network resources are not utilized properly.

Source side Protection:

The source side defense methods are deployed near the source of attack so that attacks generated are blocked at the source side itself. The source side protection methods are employed at the edge router. Ingress method and dward method [12, 13, 14] are the source side defense mechanism Ingress filtering: In this method filtering of packets based on the valid IP addresses [12]. It will filter spoofed packets sent from the client. However if the spoofed IP addresses are within the range of valid IP internal addresses then those cannot be detected. D-WARD [13,14] method monitors the incoming and outgoing packets and compares with the normal traffic flow and detects any deviations from normal traffic flow as attack. Normal traffic flow is determined by tracing the packets that behave in a normal traffic. Normal traffic is identified depending on number of SYN and ACK packets sent and received. Similarly other factors are used related to normal traffic. Normal traffic pattern is designed and by comparing the current traffic pattern with the normal traffic pattern it filters the packets. The main disadvantage of source end defense mechanisms is these needs to be implemented for all the end systems

Discussion : The attacks generated from the attacker are filtered at the source end itself and hence these packets will not go through the subnet routers and will not reach the victim. Hence the processing of these packets is done at the Source end defense mechanisms. Hence the newtwork resource utilization is good when the source end defense mechanisms are used .

Table1: Proposed Defense mechanisms ability to defend attacks and utilization of network resource

Defense Mechanism type	Defense of attacks	Network Resource Utilization
Victim side	Best practically available method to protect servers from attack. Most of the servers protect their servers using the victim side defense methods.	The network resources like routers and victim side resources are used in processing the attack packets. Hence the network resources are not utilized efficiently.
Intermediate side	It is much better method to defense the DDoS attack as many routers are involved.	The network resources like routers are used in processing the attack packets. Hence the network resources are not utilized efficiently.
Source side	It is difficult to defend the DDoS attack as it needs to be implemented on all the sources.	In these method the attack packets are filtered at the source end only. Thus these attack packets are not processed by many routers on the network. Hence the network resource utilization is good.

V. CONCLUSION

During DDoS attack large amount of packets are processed by the network resources such as routers and servers is verified practically. All the defense mechanisms are classified based on the location of the deployment. We compared the source side, intermediate router side and victim side defense mechanisms related to achieving the efficient network resource utilization and environment friendly. We suggest that the source end defense mechanisms are best as the Network IT resources are used efficiently.

REFERENCES

[1] Evans, D. (2011). How the next evolution of the internet is changing everything. CISCO White Paper, 4(11)

[2] Green IT” http://searchcio.techtarget.com/definition/green-IT-green-information-technology

[3] Ye, Terry Tao, Giovanni De Micheli, and Luca Benini. "Analysis of power consumption on switch fabrics in network routers." Proceedings of the 39th annual Design Automation Conference. ACM, 2002.

[4] Prasad, K. Munivara, A. Rama Mohan Reddy, and K. Venugopal Rao. "DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey." Global Journal of Computer Science and Technology 14.7 (2014).

[5] ostinato Network traffic generator Analyzer" http://ostinato.org/

[6] ab - Apache HTTP server benchmarking tool "https://httpd.apache.org/docs/2.4/programs/ab.html

[7] https://www.wireshark.org/download.html

[8] H. Wang, C. Jin, and K. G. Shin, Defense Against Spoofed IP Traffic Using Hop-Count Filtering, IEEE/ACM Trans. On Networking, vol. 15, no. 1, pp.40-53, February 2007

[9] Eddy, Wesley M. "TCP SYN flooding attacks and common mitigations." (2007).

[10] K. Park, and H. Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, in Proc. of IEEE INFOCOM 2001, pp. 338347.

[11] A. T. Mizrak, S. Savage, and K. Marzullo, Detecting compromised routers via packet forwarding behavior, IEEE Network, pp.34-39, 2008.

[12] FERGUSON, P. AND SENIE, D. 2000. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827. Internet Engineering Task Force (IETF). Go online to www.ietf.org

[13] J. Mirkovic, G. Prier, and P. Reiher, Attacking DDoS at the Source, in Proc. of the 10th IEEE International Conference on Network Protocols (ICNP '02), Washington DC, USA, 2002.

[14] J. Mirkovic, G. Prier, and P. Reihe, Source-End DDoS Defense, in Proc. of 2nd IEEE International Symposium on Network Computing and Applications, April 2003.