Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 11, November -2015

Performance of SNMP under A Denial of Service Attack

Dargad Sweta Arunkumar

Information and Network Security, Nirma University

Abstract — *SNMP is known as the defacto standard for Network Monitoring. It sends snmp get_requests to networking devices and in return get_response is delivered to the SNMP managing device. A SNMP based network Monitoring system creates graphs for in/out traffic of a networking device. Thus it monitors the network and trends the graphs and notifies the Network Admin of any intrusion or misbehavior in network. A denial of Service attack is when legitimate users do not get to use the network they are destined for. Under such circumstances the network monitor should notify the Network Admin. In this paper we will discuss a scenario when there is a TCP flooding based DOS attack on a network .We will see how our SNMP helps in detection of the attack and visualizing our network just by monitoring the traffic and ping statistics of the switches which were used to design the network. Also we would collect historic information for base-lining and trending Purposes. We will monitor the network using Network Monitoring System which works on SNMP and then try to get some interesting results. Thus under such circumstances we will check performance of SNMP based Network Monitor.*

Keywords- *Network Monitoring System; SNMP; MIB; Oid; RRD Tool; TCP; DOS*

I. INTRODUCTION

Due to the advancements in technology, the cost of computers has reduced. As a result, the networking infrastructure has grown. Any Network Administrator of an organization would want to have acute information of the network. He would wish to identify bottlenecks of the network as well. The person responsible to manage and monitor the network is the Network admin who requires a complete knowledge of the network. "Network Monitoring System[4] is a combination system of hardware and software, functioning as monitoring and administering tools for heterogeneous networks". "The term Network Monitoring describes the use of a system that can constantly monitor network for slow or failing components and also notify the network administrator in case of any problem".

We know that SNMP is de-facto standard for monitoring any computer network. Various open source and proprietary tools like Cacti, Nagios, OpenNMS use SNMP for data collection either to graph the network matrices or to view status of network devices. "Simple Network Management Protocol (SNMP)[1] is commonly available on all network devices". A network managed by SNMP is made up of a MANAGEMENT STATION which can be thought of as a server and a critical network device. SNMP sends SNMP get_request to the networking device using a polling system continuouslyand stores the information received in the form of MIB's. Management Information Base (MIB)[5]is a hierarchical specification of the management data on a managed network device.This information is in the raw form i.e., GAUGE[2] or COUNTERS[2] or raw text format values . SNMP can be used to get hardware and software information of all the network devices from single point of contact. Now this raw data can be made useful by creating graphs which can show the trend of network.

RRD Tool can be used to handle such raw data, it can monitor metric like bandwidth, memory usage, CPU load etc. Using RRD Tool graphing utility graphs filled with real-time[3] data can be stored in PNG format. These graphs can be easily viewed on a web browser. Thus the real-time uplink and downlink status of networking device can be viewed in a graphical format. Network Bandwidth is the metric which evaluate network path performance for small or larger transmission. Traffic monitoring on a device is very critical because if the traffic flow is not normal a sudden increase in traffic can be a trail to Denial of Service attack.

Denial of Service (DoS) attack has become a great threat for proper functioning of a computer network. The main purpose of DoS attack is to disable a service or degrade the performance of a network. DoS attack occurs when actions of single attacker results in making certain service unavailable by its target audience. Such attacks can be carried out in numerous ways, of which one is TCP flooding. TCP SYN flood attacks typically target different websites, web-servers of large organizations like banks, credit card, payment gateways, and even name servers. In TCP SYN flood attack, attackers send TCP connection request faster than a computer can process them, it sends large number of SYN packets (request) with IP spoofing techniques to the victim host and exhaust the TCP connection queue.

II. RELATED WORK

In [2], They gave a memo which has a description on the common structures and identification scheme. The definition of management information used in managing TCP/IP-based Internet is shown in this paper. The most important information from this document was about defined data-types which included Network Address, IP Address, Counter, Gauge, Time-ticks and Encoding.

In [6] They described the effect of TCP flooding, the Systems providing TCP-based services to the Internet community may be unable to provide those services while under attack and for some time after the attack ceases. They say that the service itself is not harmed, only the ability to provide the service is impaired for a specific period of time. In some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

In [7]They have done a detailed study of SYN Flooding in TCP. They described that how to do such an attack. Also how to detect the DOS attack is explained in this paper.

In[8] They have explained that the SYN flood exploits the 3-way handshaking of the TCP by sending many SYN request with IP spoofing technique to victim host and exhaust the backlog queue resource of the TCP and deny legitimate user to connect. They have captured the packet flow. Similarly we also captured the in and out traffic of the networking device interfaces.

Step1. An intruder initiates TCP SYN flooding by sending numerous connection requests with spoofed source IP Address (client) to the target machine (server).
Step2. The target machine (server) has to acknowledge the SYN message and send SYN-ACK message to the intruder. Thus the connection between the client and the server is open, and the service-specific data can be exchanged between the client and the server.

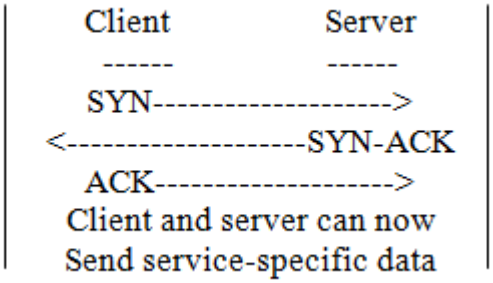

Fig 1: Client-Server Message exchange

Step3. The attack is successful when target machine has sent an acknowledgment (SYN-ACK) back to intruder machine but has not yet received the ACK message. Thus a half-open connection is created, which is the underlying vulnerability.
Step4. The intruder machine sends SYN messages to the target machine, this appear to be legitimate but in fact referred client system(genuine) was unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the target server machine.
Step5. The half-open connections will fill the data structures on the target server machine, then the system will be unable to accept any new incoming connections until the table is emptied out. Thus the legitimate user will not be able to use the service and will feel Denial of Service. Thus TCP Flooding is accomplished.

III. SYSTEM ARCHITECTURE

A. Experimental Setup:

Step1. We design a network of three switches connected to each other, say Switch-A, Switch-B and Switch-C.
Step2. We connect these switches to an external switch which is connected to 2 workstations, one of which is a server for our SNMP based Network monitoring system.
Step3. Now we monitor the switches by generating a graph of In/Out traffic on the Interface of the switches A, B and C. "***SNMP PING IP-Address***" command is used to get the ping latency of any networking device. "***SNMP get-request ifHCInOctets***" for in-traffic on an interface and ***"SNMP get-request ifHCOutOctets"*** for out-traffic on an interface of a switch.

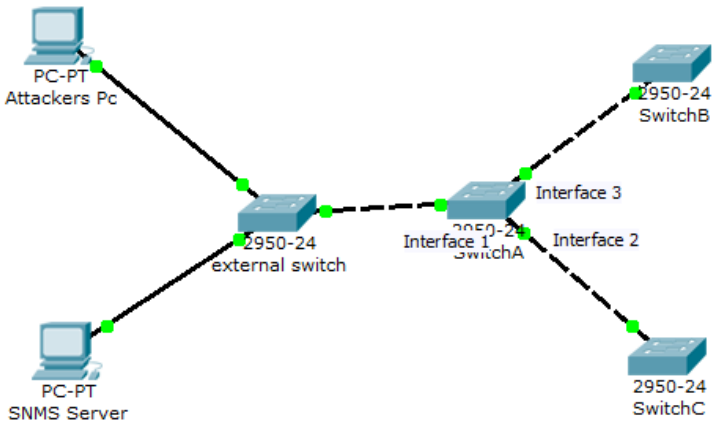

Figure 2: Network Setup

B. Objective

- To do a Denial of Service attack, we would generate a lot of traffic by TCP flooding on the switch B. As explained earlier.
- We would now grab the traffic using Network Monitoring system and see how it could point towards such an attack.
- We will analyze the Traffic graph of the switch before and after the interval of the attack.

IV. EXPERIMENTAL RESULTS

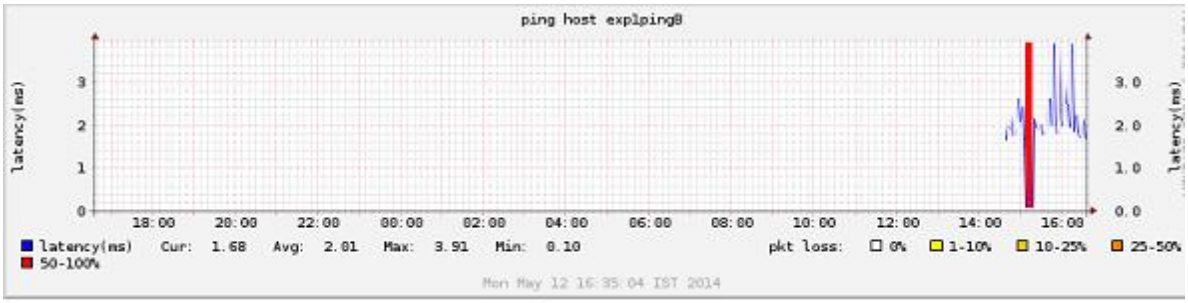

Figure 3: Graph Showing Ping Latency of switch-B

Result 1: The above figure 3 shows a graph of ping statistics of switch-B which explains that the switch was down at nearly 3pm. This is understood because the Red bar shows that there was 50%-100% packet loss. The Monitoring Server was trying to ping switch-B but it was unavailable. Latency to ping the device was 3.91, which is very low.

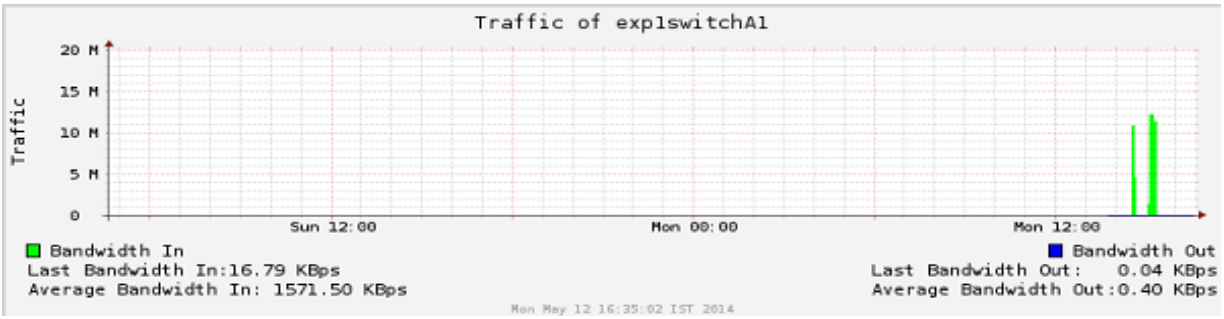

Figure 4: Graph Showing In/Out Traffic of Switch-A at Interafce1

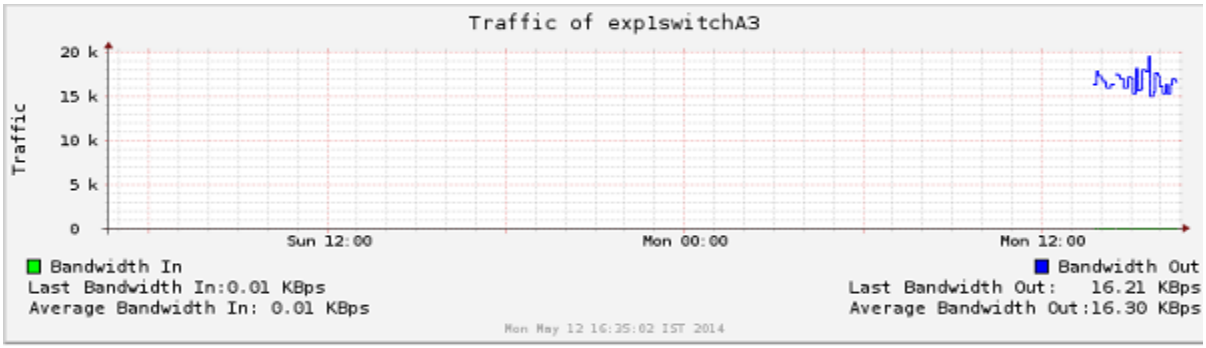

Figure 5: Graph Showing In/Out Traffic of Switch-A at Interafce3

Result 2: We can see some more interesting results. We have connected Switch-A to the external network at interface-1 and to Switch B at interface-3 as in figure 2. The graph in figure 4 shows that the In-traffic of Switch-A at interface-1was 11 Mbps approximately. But at the time of attack, the graph is seen to be empty as the SNMS server was unable to send packets in the time interval of DOS attack on Switch-B. This explains that the SNMP "get Request" to graph was unable to get the SNMP reply at the time of DOS attack. The next graph shows traffic of Switch-A at interface 3 where we can see the Out traffic only as the traffic from external network which comes to Switch-B is passing from Switch-A.

IV. CONCLUSION AND FUTURE WORK

We conclude that SNMP works as an efficient protocol for network monitoring. It is even capable of monitoring slightest change in the traffic which may be due to DOS attack. It displays very efficiently in its graphs that there is an attack and the Network Administrator is notified in time by the graphs. Thus minimum damage is done to network. The legitimate users can also be notified of the attack and proper actions can be taken by the Network Admin. Thus we can say that SNMP performs well in DoS attack.

REFERENCES

[1]D. Harrington, R. Presuhn, B. Wijnen. "RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", pp 55-60, IETF, December 2002.
[2] M. Rose, K. McCloghrie. "RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets", pp 8-12, IETF, May 1990
[3] Ranganai Chaparadza," On designing SNMP based monitoring systems supporting ubiquitous access and real-time visualization of traffic in the network using low cost tools", pp 9-12, Journal 13th IEEE International Conference on Networks,2005
[4] Authors Zeng, Wenxian Wang, Yue "Design and Implementation of Server Monitoring System Based on SNMP", pp 680-682, International Joint Conference on Artificial Intelligence and Journal 2009
[5] Paul Moceri, "SNMP and Beyond: A Survey of Network Performance Monitoring Tools", pp 2-5
[6] CERT (1996). CERT Advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks. Available at: http://www.cert.org/advisories/CA-1996-21.html. (Date of access: January 2, 2006)
[7] Christoph L. Schuba, Ivan V. Krsul "Analysis of Denial of Service Attack on TCP", pp 3-5
[8] Deepak Singh Rana, Naveen Garg, "A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations", pp 1-3 IJCTA July-August 2012 .

