An Empirical Study of Network Security System Through Dos Attack

[1]V Uma Rani[1], [2]Dr.B.Sateesh Kumar, [3]Amar Kumar Yadav
[1]Associate Professor, [2]Associate Professor, [3]M.tech Student
[1]Department of Computer Network & Information Security ,
[1]School of Information Technology (JNTUH), Hyderabad, India

Abstract: Computer network have become increasingly ubiquitous. The world has come to rely on these networks to provide transport for many different mission critical services. However, with the increase in network application, there has also been an increase in difficult for network administrator to control what traffic traverses their network, manage and secure these networks from different attacks. In computer networks, an attack is a security threat that involves an attempt to access, change, damage, reveal information without authorized access or permission. When aim of attack is only to access and get some information from your system but the system resources are not changed or destroy in any way, then it is said to be a passive attack. Active attack occurs where the attacker accesses and either change, disables or destroys your resources or data. There are different types of attacks among which a denial of service attack (Dos) is most common dangerous attacks on network. DoS is one of the active attack on networking structure which force a server to stop from servicing its clients. Network security can be defined as the “The policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources”. Failure of network security leads to major threat to various organization such as reputation loss, business loss, service interruption etc.

The objective of this paper is to demonstrate the potential damage from DoS attacks and analyze the ramifications of the damage. We will use same penetration testing approach that are used by malicious attacker in order to test network security with one difference, i.e authorization. We will analyze different firewalls and other protective systems and they role in overall security during these attacks. For testing network systems, we will simulate DoS (Denial of Service) attacks on network using GNS3. In our Lab we will be using ipv6 to configure our network.

IndexTerms: **Computer Network, Network Security, DoS Attack,Virtualization, GNS3, Firewall**

I. INTRODUCTION

With rapid increase in the usage of computer networks for storing and sharing data, security breaches and attacks on computer networks has also increased [1] at an alarming rate. Even attacks from outside has increased in the past few years. From annual survey on cyber security, it has been revealed by UK government that not only the large organization but even the small business has been badly targeted. The aim of Network security is to protect the network resources from the intruder or any harm to the hardware, software, data and in addition from interrruption of service which they provide[2]. It consists of the certain rules and method adopted to stop and monitor unauthorized access, misuse, change, or turn-down of a computer network and network assets which includes both hardware and software technologies. Good network security provide access to the network resources to authorised person or device. It focuses on different threats and stops them from passing or spreading on your network.

Computer Network Security is becoming one of the most important issues in today’s IT security world. The rapid growth of the commercialized Internet has opened up many security vulnerabilities especially due to the fact that most of the major corporations now provide web services, which often create a large part of the companies’ revenue. If these services are compromised or inaccessible, it could result major threat to various organization such as reputation loss, financial loss, business loss, service interruption etc. Nowadays, one of the most significant threat for computer network is Denial of Service attacks[2][3].

1.1 DoS Attack

Denial of Service attacks (DoS) are aimed at exhausting resources of a target, in order to make the service inaccessible for legitimate users. These attacks could have many forms, but usually they send overwhelming amounts of invalid requests to the target[4-12]. If there are multiple sources of attack, this is called Distributed Denial of Service attack (DDoS). The strength of Dos and DDoS attacks is that these attacks are very easy to perform and could have significantly negative impacts upon the target. Late development of hacktivism, from groups such as Anonymous are generally known to use DoS attacks as a part of protest .

Therefore motivations for executing DDoS attacks can vary. Nevertheless these attacks are becoming a very large problem, especially with the lack of simple and effective mitigation processes. The following are the common ways of DoS attacks [10-11] .

- The denial of service by overloading by flooding a terminal request, and to make sure that it's not able to meet the particular demands;
- The denial of service by exploitation the weakness that is exploiting a flaw of the remote system to make it unusable.

1.2 Types Of DoS Attacks

The first DOS attack occurred on November 2, 1988.This attack was self propagating & self replicating and as a result 15% of systems connected to network was stopped running and were infected. There are several kinds of DOS attacks which is generally divided into 3 categories [7]

- **Volume Based Attacks:** Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attacks aim is to overload the bandwidth of the victim site, and magnitude of attack is measured in bits per second (bps).
- **Protocol Attacks:** This type of attack **i**ncludes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. Protocol based attack overload the server resources, or it may be intermediate network device, such as router, switch, firewalls and load balancers and the magnitude of attack is measured in packets per second (Pps).
- **Application Layer Attacks:** This includes attacks that concentrate on operating system vulnerability. It includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. It is consist of request that seem genuine, the objective of those attacks is to shutdown the online server. The magnitude of this attack is measured in Requests per second (Rps).

1.3 Symptom Of DoS Attacks

Not all interruption to service are the outcome of a denial-of-service attack. There may be some technical issues with a specific network, or system administrators may be doing certain maintenance work. However, the below characteristic could indicate a DoS or DDoS attack:

- Unusually slow network performance (Opening files or Accessing websites).
- Unavailability of a particular services.
- Inability to access any websites.
- Dramatic increase in the amount of Spam you receive in your account.

1.4 Protection

Unfortunately, we do not have any perfect ways to prevent being the victim of a DoS or DDoS attack, but there are certain steps we can take to minimize the possibility that an attacker may use your computer to attack other computers [4-13]:

- Install and maintain anti-virus software.
- Install a firewalls, and configure it to restrict traffic coming into and leaving your Network.
- Install a firewalls, and configure it to restrict traffic coming into and leaving your Network.

II. RELATED WORK

Due to ubiquitous nature of computer network the world has rely on it for many critical services. Proper security mechanism are needed to ensure keeping the network available for its user. DoS vulnerabilities need to be identified to protect these network from these attack.
In this section we survey some of related research in creating virtual environment and how this can be helpful for testing network security. Our target attack was Denial of Service attack which is common now a days. There are many researchers who had done many work on network security may be after the establishment of first network, few paper related to our work are:

J loannidis and S.Bellovin, in 2002, [13] implemented mechanism on router based on pushback concept for defense against flooding attacked.

Majed Tabash and Tawfiq Barhoom, in 2014, [6] proposed an approach called DPDoS to detect and prevent DoS attacks. This approach was based on data mining technique. This approach was highly success and was able to provide 99.96% accuracy.

shamma Al Kaabi,Nouf Al KINdi,Shaikha Al Fazari and Zouheir Trabelsi , in 2016, [5] have proposed an approach to provide DoS_Vlab platform to student which will help them to learn and perform network security experiment independently and in secure environment, increase their interests on Dos attacks and improvement their understanding of network attacks concepts.

Awatef Balobaid,Wedad Alawad and Hanan Aljasim, in 2016, [7] have describe several DoS/Ddos attacks and mitigation techniques in the cloud environment. DoS attack was simulated in OpenStack Platform and attack was observed using monitoring tools like Wireshark, IP Traffic monitoring (IptTraf). To prevent Dos attack Iptables, software and hardware based firewall were used.

Gaurav Kumar, Alexander Perez, in 2017, [9] analyzed the effect of Dos attack on WLAN server with the help of jammer. When jammer was introduced to WLAN server, the time to access WLAN server by workstation was increased to 16 sec from 0.002 sec which was thousands times more than the no DoS scenario.

Kemal Hajdarevic,Adna Kozic and Indira Avdgic, in 2017, [8] represent a virtual mode using GNS3 with goal to educate large number of network administrator who don't have enough experience, tools such as intrusion detection and prevention system but who are still expected to monitor and defend computer network for which they are responsible. Different DoS attack was simulated and their behavior was observed.

III. VIRTUALIZATION ENVIRONMENT AND GNS3 SIMULATOR

The term ‘virtualization’ refers to the approach of using specialized software to conceptualize computer’s physical resources into virtual resources [13]. Those specialized software, such as Oracle’s Virtual Box, Vmware Workstation, GNS3 etc allow users to create a number of virtual machines on a user’s physical machine. Below figure depicts the architecture of the virtualized environment used to build the proposed virtual testing platform.

When deploying virtualization, [5] the user’s physical machine is known as the host machine and its operating system is addressed as the host operating system. This is illustrated in below figure, as the layer above the “Shared Hardware”. The host operating system supports the creation of several virtual machines (VMs). For instance, a user could install a Linux based virtual machine and a Windows based virtual machine on the physical machine where both the Linux based virtual machine and the Windows based virtual machine are referred to as guest operating systems. This is reflected in as the layer above the “Virtual Box” layer. The installed VMs are treated as complete instances and as actual operating systems that share the physical resources of the host operating system without intervening with the host machine in anyway.

To study Dos attack we will use GNS3 network simulator [6]to build network topologies for implementing lab for Dos attack. The reason for this choice is that GNS3 ,it allows us to visualize, plan, experiment and investigate network environment across any vendor platform at scale-without using network hardware. With the graphical interface,users can seamlessly connect all types of virtual interfaces to compose a real representation of networks. GNS3 runs on traditional PC hardware and may be used on multiple operating systems, including Windows, Linux, and MacOS X.

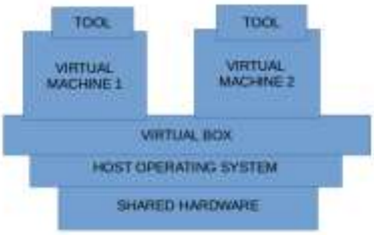


Fig. Virtualization environment

3.1 BENEFITS OF VIRTUAL TECHNOLOGIES FOR NETWORK SECURITY EDUCATION

Virtualization offers potential opportunities and benefits [5] in an network security educational setting, including creating a virtual sandbox for risky activities, providing instruction in various applications or operating systems, using virtual appliances, using virtual teams for client/server applications, and enabling distance education via virtual desktop infrastructure .

Virtualization technologies are ideally suited for providing a sandbox for executing risky code or engaging in ethical hacking experiments. In fact, students may perform ethical hacking actions on the virtual machine that they should not perform on a physical machine as these actions pose a threat to the availability and stability of the physical machine. Students may engage in activities in a virtual machine that information security educators and network administrators would not want them to do on a host machine or live network. For example, students in hands-on lab exercises cracked passwords in their virtual machines. Since the virtual machine is limited in scope in terms of this activity, real user information on the host machine and network remained secure. Students also experimented various applications, such as firewalls, intrusion detection systems, vulnerability scanning tools, hacking tools (such as DoS attack tool), virus scanners, encryption applications, to name a few, which have the potential to weaken security if not properly implemented.

IV. EXPERIMENT SETUP AND USED HARDWARE AND SOFTWARE COMPONENTS

To simulate the dos attack presented in this paper,we used network management simulator tools GNS3 which can use a to design high quality and complex network topology. It can emulate many cisco router platforms and PIX firewalls and can connect the simulated network to the real world.

In our lab we have created three different network scenario. First one without any security appliance (fig 4.1),second with sophos UTM HomeEdition 9.358 (fig 4.2) and the last is with cisco ASA 9.8.1 (fig 4.3). Apart from those security appliance our lab consist of web server ,network monitoring server (prtg),attacker machine (kali) and few client machine which access the web page. Our web server and the attacker system is in different subnet (network).we simulated Denial of Service (Dos) attack to the web server by flooding tcp, udp and http packets from the attacker machine,which is ,in this case ,our virtual machine. Furthermore ,we analyzed the page loading time ,full page loading time and download bandwidth in the client system ,considering the following cases:

a)Without security appliance and all the normal traffic is passing through to the server.

b)Flooding the server with tcp,udp and http packets without protecting the web server with any security appliance.

c) Flooding the server with tcp ,udp and http packets while using sophos Utm HomeEdition 9.358

d) Flooding the server with tcp ,udp and http packets while using cisco ASA 9.8.1

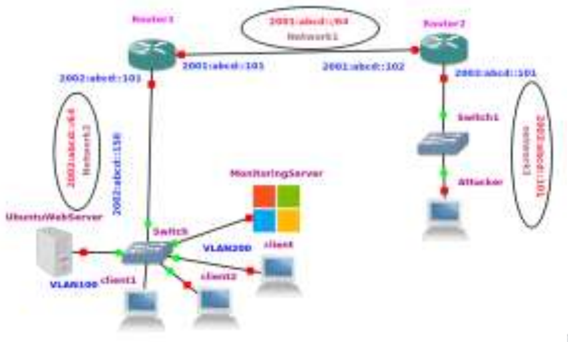


Fig 4.1 (Without security appliance)

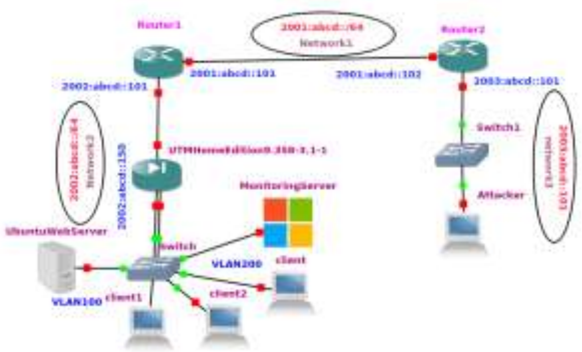


Fig 4.2 (protecting with sohpos Utm)

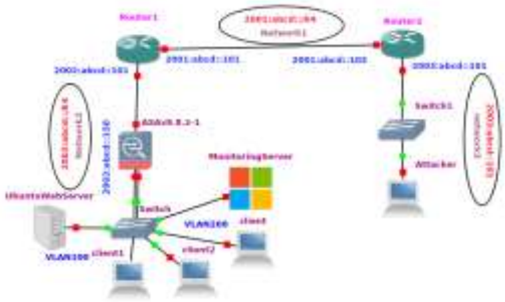


Fig4.3 (with cisco ASA)

4.1 Hardware and software components for our experiment

To perform simulation we have use ubuntu 16.04 as host machine with 8 GB RAM and processor Intel(R) Core(TM) i5-5200U CPU @ 2.20GHZ .we have used Vmware WorkStation and installed kali linux and ubuntu webserver in it .We have also installed attaking tool LOIC (Low Orbit Ion Cannon) in kali linux and setup apache virtual host in webserver.we have installed windows server 16 (QEMU) in GNS3 which has PRTG installed .PRTG is used for monitoring the network.we used virtual machine to protect our computer from the potential threats during the Dos attack simulation which was done using LOIC.

Furthermore,we installed GNS3 2.1.8 on our host machine.GNS3 software enables building simple and complex virtual networks without having physical devices,such as router and switches,to simulate real network components.To do so ,we used emulators such as Dynamips and Qemu and created software equivalent fo hardware devices.Furthermore ,GNS3 can be connected to the external virtualmachines or physical devices , that provides creating more complex network topologies and simulation of real scenarios.

GNS3 needs real cisco IOS images to emulate cisco router and other devices.In our simulation ,we used 3745 and 7200 series router.Furthermore,we used the IOS image c3745-advipservicesk9-mz.124-25d and c7200-advipservicesk9-mz.152-4.S5 for 3725 and 7200 series router respectively.Each router require specific Ram memory.Minimum memory for router c3745 is 256MB and for c7200 is 512MB.

Morever ,we used Cisco Sophos UTM HomeEditiion 9.358 and cisco ASA 9.8.1 firewall each with 1GB RAM as it is sucurity device that combines firewall,antivirus ,intrusion prevention and virtual private network (VPN) capabilities and we belive it is a good security mechanism for attack prevention.we have used each device once and checked the performance of each device during the dos attack.

4.2 Attacking tools used in experiment

In our experiment ,we have used above mentioned LOIC tool (fig 4.4) ,which is an open-source GUI tools used for network testing and Dos attack application written in c#.It can be used for different dos attack like tcp flood,udp flood, icmp flood,http flood etc.Even though LOIC have many option we have only used tcp ,udp and http flood in our experiment.The GUI interface of LOIC tool is show in fig 4.4

LOIC performs a Dos attack on a target site by flooding the server with tcp or udp packets with the intentiion of disrupting the service of a particular host. LOIC is easy to use.Attacker just need to lock the target either using url or its ip ,then select the type of attack .we can select number of threads we want to send and control the speed of the packets sent.

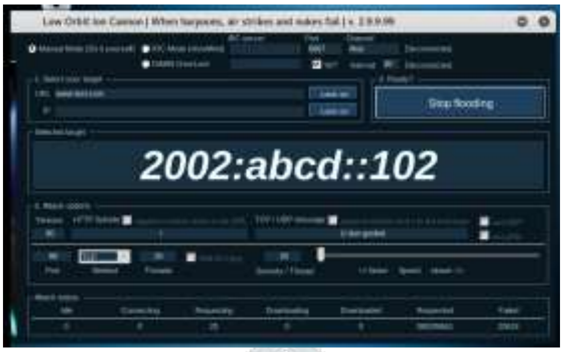

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v. 2.9.9.99
Stop flooding
2002:abcd::102

Fig 4.4

V. NETWORK SIMULATION AND RESULTS

We setup and was ready for simulation. All the device were switch on and we simulated our network in all four cases that we have mention. The result was recorded and was compared with each other.The simulation result of all cases are as follows-

5.1 Without security appliance and all the normal traffic is passing through to the server.

In the first scenario,we have not used any security appliance to protect our networks so all network traffic can pass through it to server .Even our network is not under any attack. After all device are setup and connected to a topology as shown in fig 4.1 we tested the connectivity between client and server. All the client were allowed to access the website normally. The test was carried out for few hours and at the same time ,monitoring the network with PRTG..The average loading time ,download bandwidth and average loading time of full websites in client system was 16 msec ,2778 Kbit/s and 646 msec respectively. The observation is show in fig 5.1 and fig 5.2 .

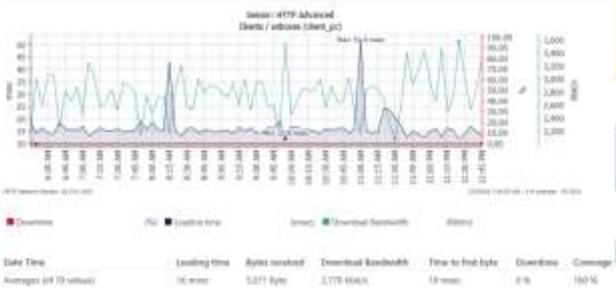


Fig 5.1

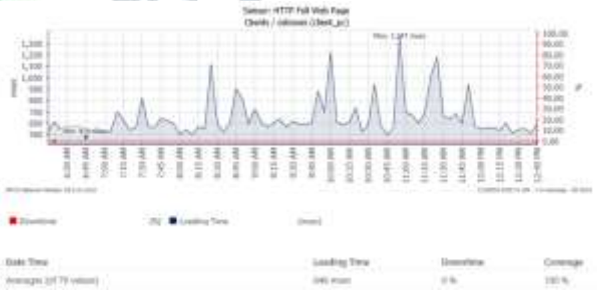


Fig 5.2

5.2 Flooding the server with tcp,udp and http packets without protecting the web server

In second scenario ,we lunched a Dos attack on web server .we lunched three different type of Dos attack ,tcp flood,udp flood and http flood.In this scenario also the web server was not protected with any security appliance. There was vast difference in the loading time of web page in client system when tcp and http flood attack was lunched. where as in case of udp flood there was not much change. The observed data is given in below table 5.1 and graph is show in fig 5.3 and 5.4.

	TCP	UDP	HTTP
Average loading time	70 msec	21 msec	41 msc
Download Bandwidth	1199 Kbit/s	2589 Kbit/s	1345 Kbits
Full page loading time	1416 msec	2027 msec	1476 msec

Table 5.1

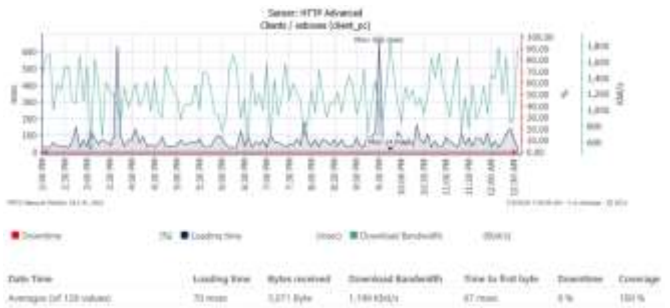


Fig 5.3

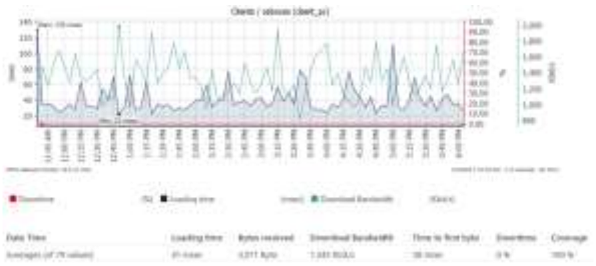


Fig 5.4

5.3 Flooding the server with tcp ,udp and http packets while using sophos Utm HomeEdition 9.358

The third case is similar to that of case 2 with only difference is that we have used security appliance cisco sophos Utm homeEdition .During this test we have tried to find the efficiency of this appliance
from Dos attack. The same attack which as mention above was lunched and client system was observed. we found that cisco Utm HomeEditiion 9.358 was able to defend the server from dos attack to some extend but not completely. Even though it was configured to limit the number of packets per second to minimum, it was not able to block all flooding packets. The observed data is given in below table 5.2 and graph is show in fig 5.5 and 5.6.

	TCP	UDP	HTTP
Average loading time	35 msec	19 msc	23 msc
Download Bandwidth	1596 Kbit/s	2780 Kbit/s	3037 Kbit/s
Full page loading time	1095 msec	1067 msc	2025 msc

Table 5.2

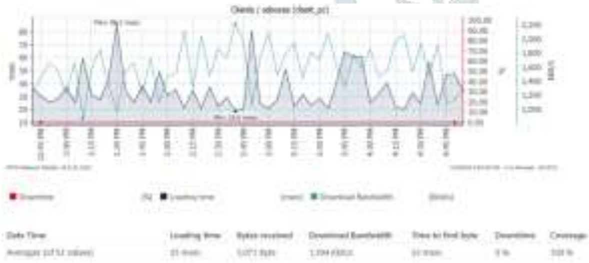


Fig 5.5

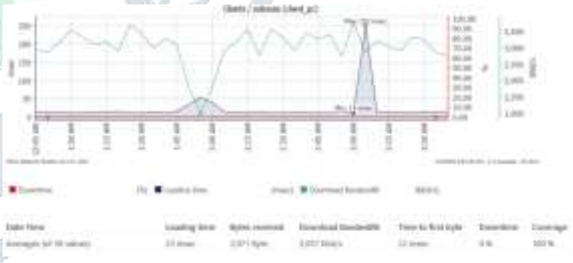


Fig 5.6

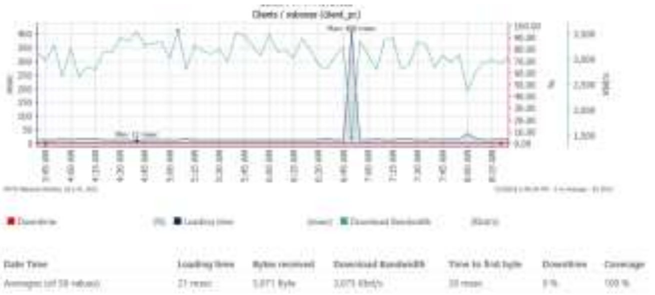
5.4 Flooding the server with tcp ,udp and http packets while using cisco ASA 9.8.1

In the final scenario ,we have used the cisco ASA firewall and set the filter and defining which connection and how many connection per client could be established. We configured ASA firewall by limiting the total number of Embryonic connection,Half-closed connection,Maximum Per-client -embryonic connection ,maximum number of simultaneous connection per client. If those limit are reached ,then the ASA firewall responds to every SYN packets,originally sent to the server with SYN ACK and does not pass the SYN to the server. If the sender responds with ACK packet ,then the ASA firewall recognized it as not a pat of Dos attack,rather a valid request. Then finally firewall establishes a connection with a web server. The observed value from client system in given in below table 5.3 and graph is show in fig 5.7 and 5.8 .

	TCP	UDP	HTTP
Average loading time	21 msec	18 msec	15 msec
Download Bandwidth	3075 Kbit/s	2800 Kbit/s	2800 Kbit/s

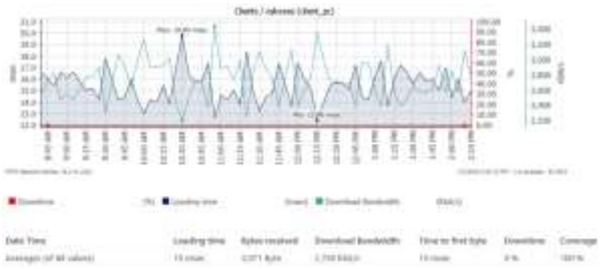
Full page loading time	617 msec	696 msec	696 msec

Table 5.3



Date Time	Loading time	Bytes received	Download Bandwidth	Time to first byte	Downtime	Coverage
Averages (of 58 values)	21 msec	5,071 Byte	3,075 Kbit/s	20 msec	0 %	100 %

Fig 5.7



Date Time	Loading time	Bytes received	Download Bandwidth	Time to first byte	Downtime	Coverage
Averages (of 60 values)	15 msec	2,571 Byte	1,700 Kbit/s	13 msec	0 %	100 %

Fig 5.8

V. CONCLUSION

GNS3 platform provides us with a secure and virtual laboratory environment and experimental experiences on common Dos attack. It reflects the real network environment and also overcome the problem such as resource limitation ,ethical and legal issues that we face during the experiment if done on the real physical network.

Our paper aims to research several Dos attacks and mitigation techniques. These attacks and mitigation technique are studied based on real time network. Our experiments show a form of attack which is common and well know , any new forms of Dos attack could present different symptoms. From the experiment performed ,it is concluded that when these systems are attacked by Dos they easily vulnerable,especially when the attacker use TCP flood. The effect of the attack can be minimize by implementing appropriate system for protecting against these attacks. we can use next generation firewall like ASA and Soph UTM ,but when attacker has more bandwidth then the victim network then this firewall may not be more efficient. In this case we need to continuously monitor the network traffic and identify such attack.

REFERENCES

[1] Harshita ,N Ramesh, “A Survey of Different types of Security Threats and its Countermeasures” ,International conference on Electrical,Electronics and Computer Engineering,May 2013,Mysore,ISBN:978-81-927147-3-8.

[2] Wikipedia[online] Available:https://en.wikipedia.org/wiki/Network_security

[3] Arianit Maraj,Genc Jakupi,Ermir Rogova and Xheladin Grajqevic ,”Testing of network Security Through Dos Attacks”, Mediterranean Conference on Embedded Computing (MECO),Bar, Montenegro , pp. 1-6, June 11-15 , 2017

[4] Tomar Kuldeep and Tyagi S.S , “Enhancing Netwok Security by Impleting Preventive Mechanism using GNS3”, International Conference on Reliability,Optimization and Information Technology, Faridabad, India ,pp. 300-305, February 6-8 , 2014

[5] shamma Al Kaabi,Nouf Al KINdi,Shaikha Al Fazari and Zouheir Trabelsi,”Virtualization based Ethical Educational Platform for Hands-on Lab Activities on Dos Attacks”, IEEE Global EngineeringEducation Conference(EDUCON), Abu Dhabi, United Arab Emirates, pp.273-280, April 10-13, 2016

[6] Majed Tabash and Tawfiq Barhoom,”An Approach for Detecting and Preventing DoS Attacks in LAN,”International Journal of Computer Trends and Technology(IJCTT)-Vol. 18 ,pp. 265-271, 2014

[7] Awatef Balobaid,Wedad Alawad and Hanan Aljasim,”A Study on the Impacts of DoS and DdoS Attacks on Cloud and Mitigation Techniques,2016 International Conferenceon Computing, Analytics and Security Trends (CAST), Pune, India , pp. 416-421,Dec. 19-21, 2016

[8] Kemal Hajdarevic,Adna Kozic and Indira Avdgic,”Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator”, International Conference on Information, Communication and Automation Technologies (ICAT) , Sarajevo, Bosnia-Herzegovina , pp. 1-6 , Oct 26-28,2017

[9] Gaurav Kumar,Eman Adelfattah,Johnathon holbrooks and Alexander Perez,”Analyzing the effect of Dos attacks on network Performance” , International Conference on Communication, Computing and Digital Systems (C-CODE), pp.372-376, Oct.19-21, 2017

[10] S. Sridhar,”Denial of Service attacks and mitigatiion technique:Real time implementation with detailed analysis”, 2011,SANS Institute

[11] M.Khaled,Elleithy,"Denial of Service attacks and mitigatiion technique : Analysis,Implementation and Comparison,"IIISCI journal,vol 3,no 1, pp 666-71,DOI 10.1109/LISAT 2016.7494156.

[12] N. Muraleedharan and B. Janet ,"Behaviour Analysis of HTTP Based Slow Denial of Service Attack",IEEE WiSPNET conference, Chennai, India pp. 1852-1856, March 22-24, 2017

[13] J. Joannidis and S. Bellovin, "Implementing Pushback: Router-Based Defense against DDos Attack."In Proceedings of the Network and Distributed System Security Symposium (NDSS 2002), February 2002

[14] Brutus,S.,aA.,and Locasto,M.."Teaching principles of the hacker curriculum to undergraduates," Proceeding of the 41th ACM tecchnical symposium on Computer Science education,ACM SIGCSE,pp122-126,2010