Testing of Network Security Systems Through DoS Attacks

Arianit Maraj
Faculty of Computer Sciences, AAB College, Prishtina, 10000, Kosovo

Genc Jakupi
Faculty of Computer Sciences, AAB College, Prishtina, 10000, Kosovo

Ermir Rogova
FSHMN, University of Prishtina, Prishtina, 10000, Kosovo
Correspondence: ermir.rogova@uni-pr.edu

Xheladin Grajqevci
Faculty of Computer Sciences, AAB College, Prishtina, 10000, Kosovo

Abstract - **Cyber attacks are becoming more and more sophisticated, obtaining access to sensitive data. These attacks are causing major damages to various organizations, such as financial losses, service disruption etc. In this paper, we will use Penetration testing technique in order to test network security. This technique uses the same tools and methods as malicious attackers use, in order to take control of different systems, with one difference; These tests have been officially authorized and sanctioned. The practical part of this paper will analyze firewalls and other protective systems and they role in overall security during these attacks. Firewalls that will be analyzed in this paper are Threat Management Gateway (TMG 2010), Adaptive Security Appliance (ASA) as well as Next Generation Firewalls. For testing such systems, we will simulate DoS (Denial of Service) attacks.**

Keywords: *Cyber Attack, Penetration testing, Firewall, DoS*

I. INTRODUCTION

Recently, the number and the importance of electronic services in Kosovo have increased exponentially. With the increase of the importance of these systems, they will likely be subject to different and sophisticated cyber attacks. Therefore, there is a constant need to pay attention to defense systems in order to prevent attacks which can jeopardize the quality of such services. Cyber attacks continue to grow exponentially worldwide. There is a variety of cyber attacks such as: device compromise, service disruption, Injection of bad data, etc. [1-3]. DoS attack is considered to be one of the most dangerous cyber attack in the computer world. The aim of DoS attack is to overload and crash important networks by flooding it with useless traffic. Through DoS attack, the attackers try to prevent legitimate users to have access to different data or services such as: emails, access to web sites, etc. During this process the attacker sends a huge number of requests to the server which provides specific services. The servers have limitations on handling simultaneous number of requests. During DoS attack, the server has a hard time processing so many requests at the same time. Thus, the legitimate users might not be able to have desired services [4-5].

In this paper, we use penetration testing technique for simulating DoS attacks in order to verify the level of security systems implemented in the government network of Kosovo. We will simulate different scenarios for different types of Firewalls and we will try to come up with important suggestions for improving protective security system in the Government network. We will assume that the attacker is attacking from local network and from Internet (outside the network). We will see how DoS attacks affect up-and-running web services, which are located in a test server inside this network.

II. PENETRATION TESTING TECHNIQUE

Penetration testing is a method that simulates an attack in order to verify the security holes of a particular system. This test can be performed using hardware or software tools, but also through social engineering. The main purpose of this method is to examine the behavior of a particular system during an attack from inside or outside an Organization. The penetration testing process includes gathering detailed information regarding the target system, identifying entry points (or back doors) and reporting the findings [6-9]. The main difference between a malicious attacker and a pen-tester is authorization. The pen-tester, initially should obtain written consent from the owner of the network or system to be tested and then start testing. After completing the test, the pen-tester is obliged to write a report about the vulnerabilities found on the network and give instructions for preventing from such attacks [9]. Testing of network security is a wide area, thus there are different types of penetration testing. Depending on the information that pen tester has regarding one system, penetration testing can be:

- White box testing: pen-tester has all the information regarding testing system
- Gray Box testing – pen-tester has only partial information regarding the testing system
- Black Box testing – pen-tester has no information regarding the testing system

Depending on the information that pen-tester has regarding the domain of testing, penetration testing can be done from inside or outside network of the organization.

III. TESTING OF SECURITY SYSTEMS IN THE GOVERNMENT NETWORK

In this section we describe the testing of the security systems in government network. We will see if these security systems are able to afford DoS attacks. Since we have prior knowledge regarding the network configurations, we will use White Box penetration testing. We will use 2 different scenarios:

1. Scenario 1: A web server attack from the Local area network

978-1-5090-6742-8/17/$31.00 ©2017 IEEE

2. Scenario 2: A web server attack from Internet. The web server is protected with different firewalls
    - Scenario 2a: ASA and TMG 2010 firewalls
    - Scenario 2b: Next generation firewall - Sophos UTM

There are various types of DoS attacks, but in this paper we will perform tests using TCP and UDP flood. TCP flood attack's aim is to over-utilize the CPU of the server. When a host tries to connect to a server, a three way handshake protocol needs to be established before data transfer occurs. The host sends a SYN packet, the server replies with ACK (Acknowledgement) and finally the host should send a SYN ACK packet to create a successful connection with the server. The attacker's aim is to leave somehow this handshake process open, by not sending the SYN ACK from host to the server. Such state is saved in server's memory waiting for the host to reply. When there are a lot of such open states, the server might run out of memory. Thus, it will not able to serve legitimate clients [5]. UDP flooding is similar to ICMP (Internet Control Message Protocol), but UDP packets are bigger compared to ICMP hence it consumes RAM memory faster. Therefore this attack is very dangerous and the security experts should pay particular attention to it. There are a lot of tools freely available on the Internet which can be used for performing flooding attacks on server [10]. In this paper we will use LOIC (Low Orbit Ion Canon) tool for performing DoS attacks. The usage of this tool is allowed only for testing purposes. The use for any other purposes is prohibited by law. As a target for the attack we have created a web page for testing purposes, http//10.153.3.88, in order to not affect live services in government institutions.

IV. WEB SERVER ATTACK FROM LOCAL NETWORK-1ST SCENARIO

In order to perform this test, first there is a need to create a test environment. The Web page is installed in a virtual platform, where as an operating system is used Fedora Linux (Fig. 1).

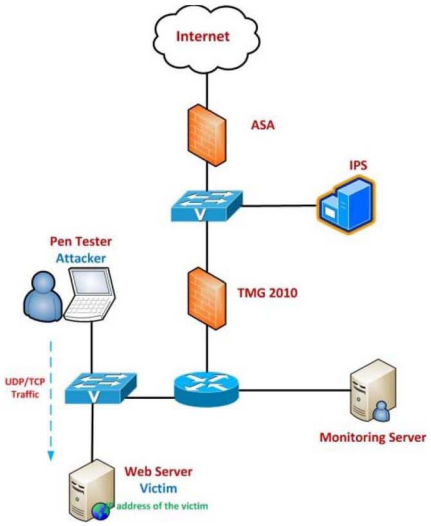
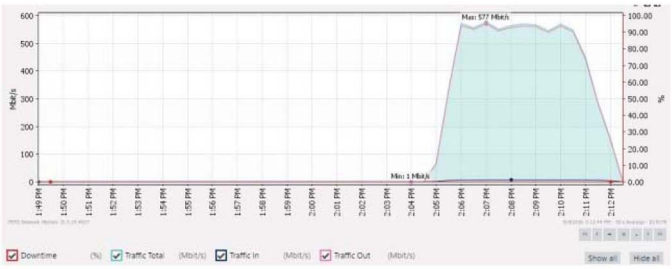


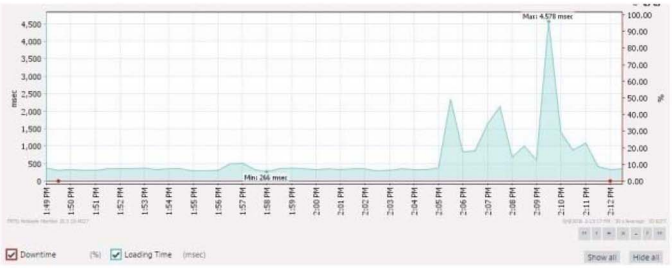
Figure1. Network topology during DoS attack from LAN

LOIC is installed in the attackers' PC (Pen-tester). Network cards installed in Server and in PC are Giga Ethernet. To monitor the server during the attack, we will use PRTG (Paessler Router Traffic Grapher) installed in another server, used for monitoring purposes. This application is configured to measure the traffic in network cards as well as the page loading time in client's browser. Before starting the attack, the attacker should check which ports are open on the server, in order to carry out the attack on those ports. Using nmap (network mapper) tool, we identified that the only port open is port number 80 (TCP).

First, the test is performed from a single PC by TCP flood (approximately 330 Mb/s). From this attack, we noticed that the page loading time is the same as it was before the attack. TCP flood from a single PC did not affect the functioning of the web server. Therefore, we increased the number of PC-s to four, generating TCP packets on port 80. The results from this test are shown in Fig.2.



a) Network Card Traffic of the web server – 4 PCs



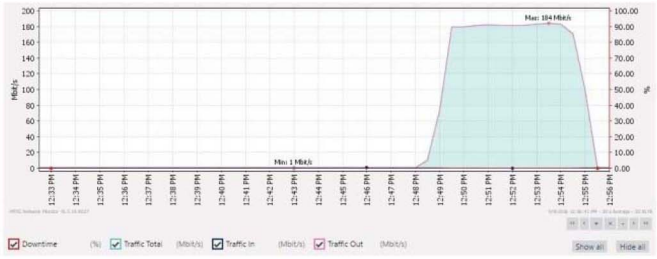
b) Page loading time, attack performed from LAN - 4 PCs

Figure 2. Results after attack from 4 PCs; TCP flooding

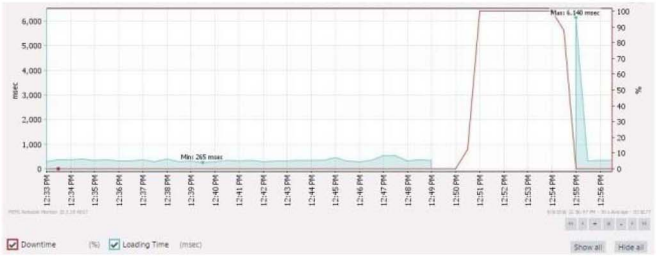
From Fig. 2, it can be seen that the traffic generated from four PCs toward the Web Server has achieved maximum 577 Mbps. Theoretically, if one PC can generate 330Mbps, then four PCs should generate approximately 1Gbps, but in this case that was not achieved. From Fig. 2.b, it can be seen that the page loading time is increased from 256 msec (before attack) to 4.578 sec during the attack. From these results, we can see that by TCP flooding it is hard to stop functioning of web pages, but if you generate a huge amount of traffic using a lot of PCs, there is a possibility to cause considerable delays on page loading.

Next we tested the functionality of Web server by flooding UDP on port 80. The port 80 with UDP is not open, but knowing that UDP is connectionless, the attacker sends packets and do not expect any response. From the results shown in

Fig.3 we can see that attacker has sent only 184Mbps. But, this traffic was sufficient to stop the page from opening.



a) Network Card Traffic of the web server



b) Web page opening time from internal network, UDP

Figure 3.Results after attack from a single PC by UDP flood

Therefore, we can conclude that by using UDP flood an attacker can very easily stop the opening one page, even if this attacker is using a single PC for committing the attack.

V. WEB SERVER ATTACK FROM INTERNET–2ND SCENARIO

i. Scenario 2a- ASA and TMG 2010 firewalls

In this scenario, the web server will be protected by 2 firewalls (ASA and TMG 2010) and the attack will be done from Internet (outside the government network).

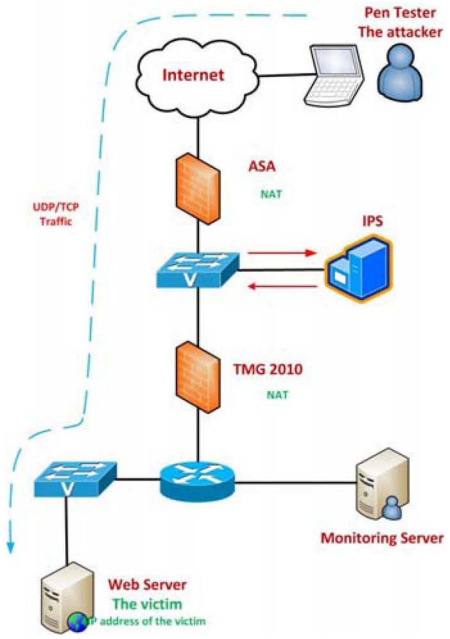
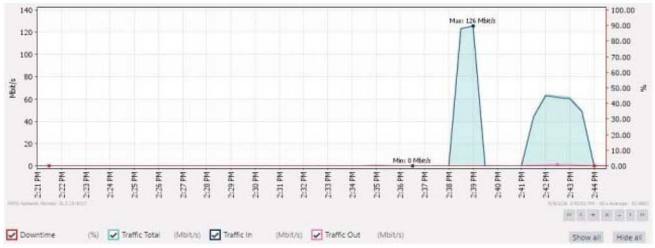
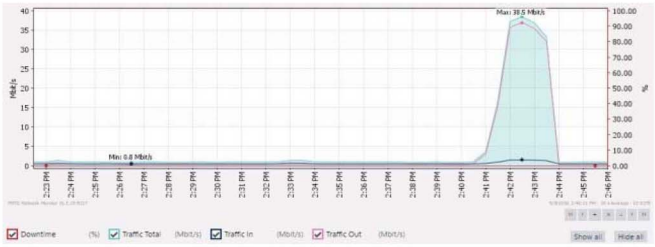


Figure 4. Government Network topology- DoS attack from Internet

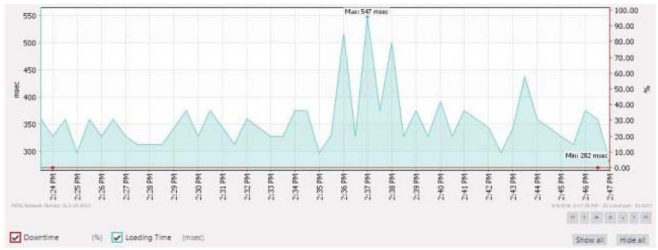
The network topology for this scenario is shown in Fig.4. This is the real topology implemented in government network. Like in the 1st scenario, we performed penetration testing by flooding TCP and UDP on port 80. The results after DoS attack by TCP flooding can be seen in Fig.5. In this case we monitored the attacker's network card, since we needed to know how much traffic the attacker sent, in order to know what the role of firewalls in this communication is. The test was done when the firewalls have been processing regular user's traffic. From Fig. 5, it can be seen that the attacker sends approximately 60 Mbps traffic towards the web server, while at the web server only 38.5 Mbps has arrived. From this it can be observed that the firewalls are doing their job at filtering the traffic. This attack does not affect the page loading time.



a) Traffic from network card of the attacker PC



b) Traffic from network card of the web server



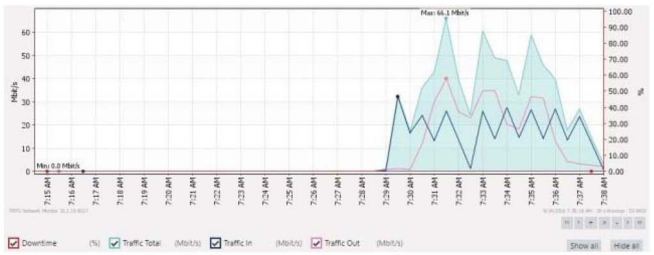
c) Web page opening time from Internet

Figure 5. Attacking the security systems from Internet through TCP Protocol

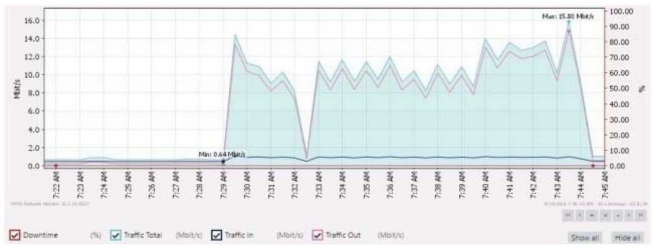
In order to understand what happened with firewalls during the attack, we have monitored their work and we noticed that after approximately 30 seconds, the ASA firewall has blocked the attacker's IP address. TMG firewall has not responded because the filtering was done by ASA, located before TMG. In order to test the behavior of TMG firewall during the DoS attack, by flooding TCP on port 80, we will next bypass the ASA firewall.

From the results presented in Fig.6, it can be seen that the traffic sent from the attacker has achieved a maximum of 35 Mbps, whereas the traffic arrived to the web server is 15 Mbps.

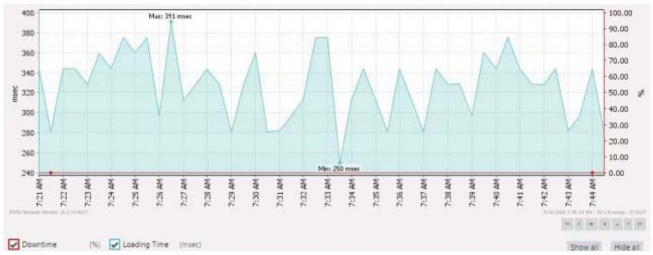
From these results it can be observed that the TMG does not fully block the attackers' IP address.



a) Traffic from network card of the attacker PC



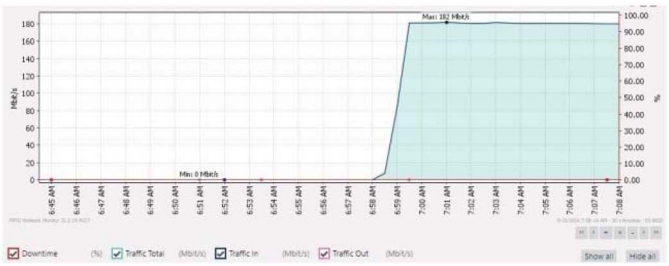
b) Traffic from Web server card



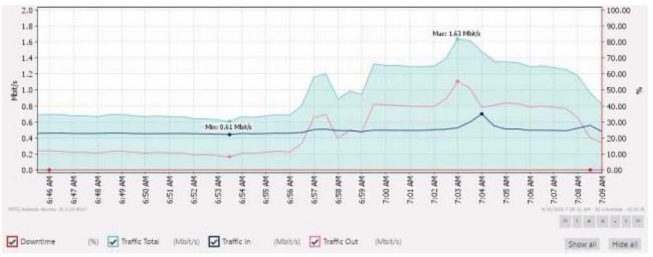
c) Web page opening time from Internet

Figure 6. Attack by TCP protocol from Internet, bypassing ASA

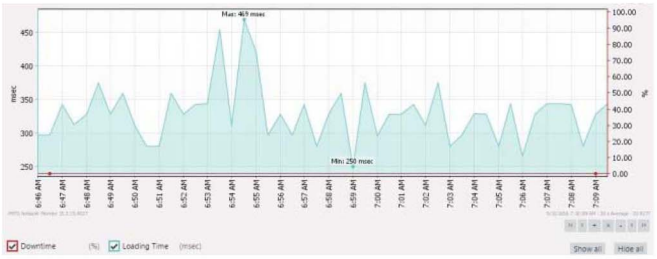
When the attacker sends UDP packets towards the web server, these packets are blocked from ASA. In Fig.7 are shown the results of the attack with UDP, where the attacker sends 182 Mbps. These packets have not reached the final destination because ASA firewall has stopped this traffic. During this attack, the processing power of ASA firewall started to grow and the traffic has been stopped almost completely from ASA.



a) Traffic from the attacker's PC



b) Traffic from network card of the web server



c) Web page opening time from internal network, UDP

Figure 7. Results of attack through UDP protocol from Internet

During this attack all services that are accessible from the Internet have stopped. The attacker was connected outside the firewall and has utilized the maximum capacity of 1 Gbps since the traffic has not passed through ISP equipment.

ii. Scenario 2b -Next generation firewall –Sophos UTM

Next generation firewalls are an advanced version of traditional ones, with many integrated functionalities, such as: web protection, server protection, email protection, intrusion prevention, endpoint protection, etc. To perform penetration tests and to analyze the difference between existing and next generation firewalls we have chosen Sophos UTM firewall. The topology of this scenario is shown in Fig.8.

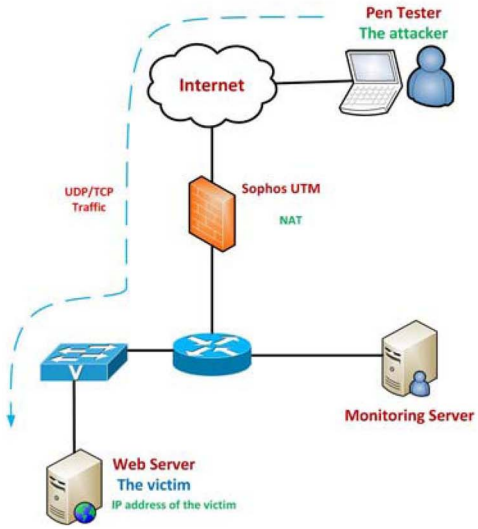
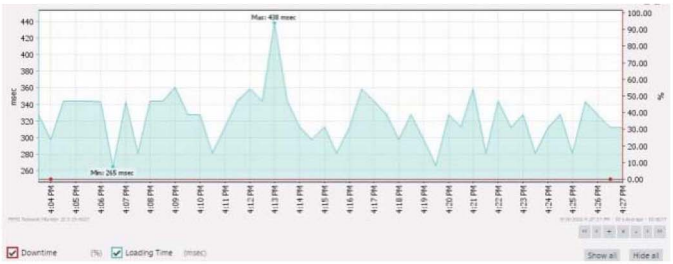


Figure 8. Network topology during testing the Sophos UTM Firewall

Like in previous scenarios, we performed penetration testing by flooding TCP and UDP on port 80. Results of TCP flood attack for this scenario are shown in Fig.9.

a) Traffic from attacker's PC

b) Traffic from web server

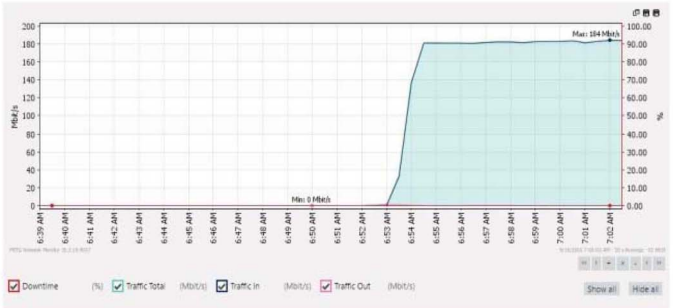


c) Page opening time - TCP flood, scenario 2b

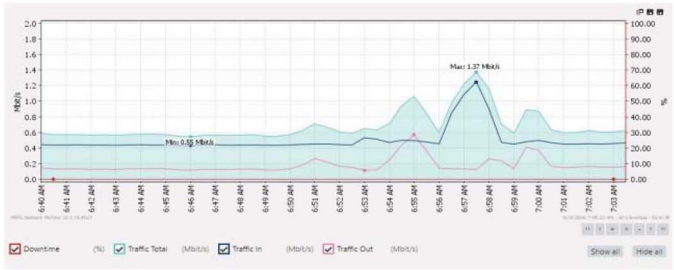
Figure 9. DoS attack results through TCP Protocol-UTM Firewall

Pen-tester sends 212 Mbps toward the web server, whereas the web server has not been seen reaching a greater number of packets compared to the time before attack. The same thing is noticed for the page loading time, so there were no delays. This firewall has achieved to stop traffic which was send by the pen-tester. This firewall did not block the attackers' IP address (it just identified it), but managed to protect the web page by discarding the huge amount of requests from the attacker.

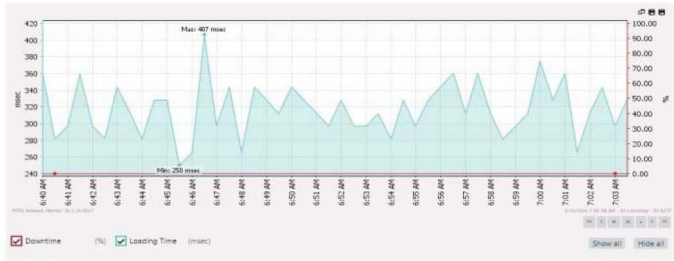
In addition, we tested security issues of UTM by flooding the web server with UDP. The results are shown in Fig.10.



a) Traffic from the attacker's PC



b) Traffic from web server

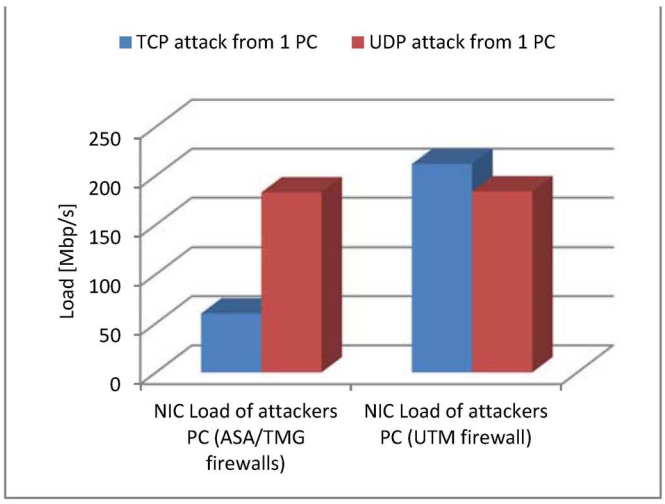


c) Web page opening time from internal network, UDP

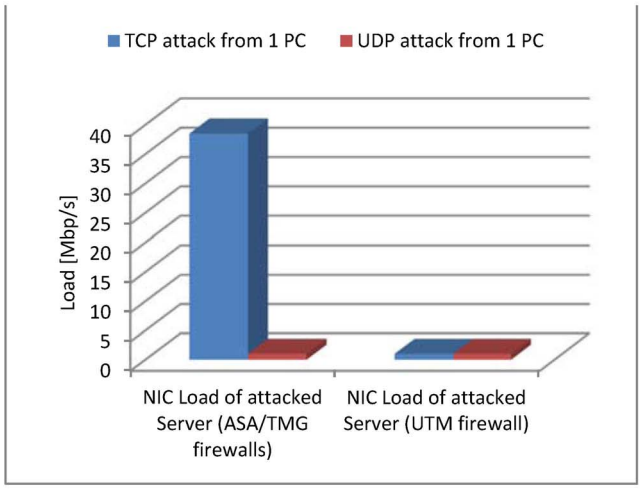
Figure 10. DoS attack results by UDP Protocol-UTM Firewall

The difference between standard ASA firewall and UTM, is that the UTM can process traffic even during the attack. So the web page remains functional even during the attack.

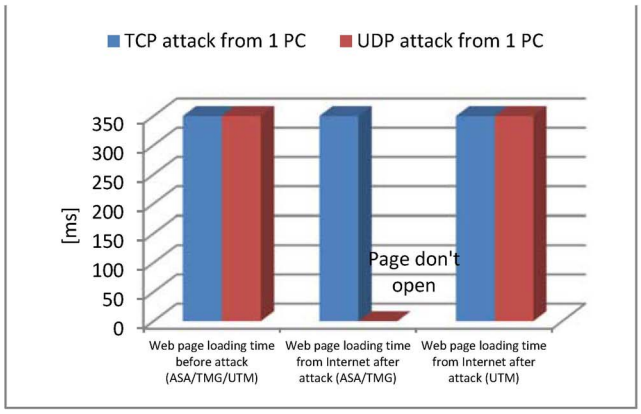
In Figure 11 (a, b, c), we will show the comparison between sub scenarios 2a and 2b, for all firewall types, considering UDP and TCP traffic.



a) Traffic from NIC card of the attacker



b) Traffic from Web Server Card



c) Web page loading time before and after attack

Figure 11. Comparison results for scenario 2a and 2b

VI. CONCLUSIONS

From the tests performed on security systems implemented in government network, it has been concluded that when these systems are attacked by DoS they are vulnerable, especially when the attacker uses UDP flood. This problem can be avoided by implementing appropriate systems for protection against these attacks. One of the alternatives is using next generation firewalls, which are capable in neutralizing such attacks, but not in the case when attacker has more bandwidth than the bandwidth that the government utilizes. In order to avoid such an attack, there is a need to continuously monitor the network and identify such attacks (IP address of the attacker). In addition, since it is very easy to interrupt services from the internal network, there is a paramount need to protect the servers with the next generation firewalls.

REFERENCES

[1] Security TechCenter. (2014, April 8). "Microsoft Security Bulletin MS14-017 – Critical". URL: https://technet.microsoft.com/enus/library/security/MS14-017?f=255&MSPPError=-2147217396 (retrieved 4 January, 2017)

[2] C.Anley, J. Heasman, F. Lindner, G. Richarte "The Shellcoder's Handbook: Discovering and Exploiting Security Holes". 2007. Wiley

[3] T. Hayajneh, B.J Mohd, A. Itradat, ANQuttoum "Performance and Information Security Evaluation with Firewalls," International Journal of Security and Its Applications, SERSC, Vol. 7, No. 6, pp 355-372, 2013.(DOI: 10.14257/ijsia.2013.7.6.36)

[4] S. Sridhar, "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis", 2011, SANS Institute

[5] M.Khaled, Elleithy, "Denial of Service Attack Techniques: Analaysis, Implementation and Comparison, "IIISCI journal, vol 3, no 1, pp. 66-71]

[6] M. Denis, C. Zena, T. Hayajneh, "Penetration Testing: Concepts, Attack Methods, and Defense Strategies, , ISBN: 978-1-4673-8490-2, DOI: 10.1109/LISAT.2016.7494156

[7] D. Piscitell, "Your First Penetration Test"Watch Guard Live Security. http://www.corecom.com/external/livesecurity/pentest.html (retrieved 11January, 2017)

[8] Penetration Testing: Assessing Your Overall Security Before Attackers Do SANS Institute, June 2006

[9] W. Georgia, P. V. Eeckhoutte. "Penetration Testing". NoStarch Press Inc., 2014. Print.

[10] J. Hatche, "Hacking: Hacking For Beginners and Basic Security: How To Hack", ISBN-10: 1517271835, 2015