computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

USING GRAPHIC NETWORK SIMULATOR 3 FOR DDOS ATTACKS SIMULATION

Anatoliy Balyk [1], Mikolaj Karpinski [2], Artur Naglik [2], Gulmira Shangytbayeva [3], Ihor Romanets [4]

[1] Ternopil Ivan Puluj National Technical University, 56 Ruska St, 46000 Ternopil, Ukraine, vodinn@gmail.com, http://tntu.edu.ua/?p=en/home
[2] University of Bielsko-Biala, 2 Willowa St, 43-309 Bielsko-Biala, Poland, mkarpinski@ath.bielsko.pl, artur.naglik@gmail.com, http://www.eng.ath.bielsko.pl/
[3] K. Zhubanov Aktobe Regional State University, 34 A.Moldagulova St, 030000, Aktobe, Republic of Kazakhstan, shangytbaeva@mail.ru, http://arsu.kz/en
[4] Ternopil National Economic University, 11 Lvivska St, 46009 Ternopil, Ukraine, irom@tneu.edu.ua, http://nncit.tneu.edu.ua

Abstract: Distributed Denial of Service (DDoS) attacks are still one of the major cybersecurity threats and the focus of much research on developing DDoS attack mitigation and detection techniques. Being able to model DDoS attacks can help researchers develop effective countermeasures. Modeling DDoS attacks, however, is not an easy task because modern DDoS attacks are huge and simulating them would be impossible in most cases. That's why researchers use tools like network simulators for modeling DDoS attacks. Simulation is a widely used technique in networking research, but it has suffered a loss of credibility in recent years because of doubts about its reliability. In our previous works we used discrete event simulators to simulate DDoS attacks, but our results were often different from real results. In this paper, we apply our approach and use Graphical Network Simulator-3(GNS3) to simulate an HTTP server's performance in a typical enterprise network under DDoS attack. Also, we provide references to related work.

Keywords: *GNS3;DDoS attack; network simulator.*

1. INTRODUCTION

Despite over a decade of research into DDoS attack detection ([1], [2], [3]), mitigation ([4], [5], [6]), and advanced source detection ([7], [8], [9]), these attacks are still one of the most dangerous threats to computer networks. Modern DDoS attacks can vary in size from several PCs to huge botnets consisting of tens of thousands of PCs from all over the world. The DDoS attach on Russian banks in 2016 was carried out by a huge botnet. Being able to model DDoS attacks is helpful in developing new techniques for mitigating them. Modeling DDoS attacks [10]-[12] in real life is not an easy task. For one thing, one must select the approach for modeling attacks. In our previous work [15] we surveyed the main approaches in this area. One can model DDoS attacks using either a specialized testbed or network simulator software. In this paper we will concentrate on the last and the most affordable option. The rest of this paper is organized as follows: in Section II we provide an overview of related work, in Section III we justify our choice of network simulator, Section IV describes the simulation, and conclusion is in Section V.

2. RELATED WORK

A performance comparison of network simulators can be found in [17]. In [17], the authors focus on the open source simulators NS2, NS3, OMNeT++, JiST, and SimPy, and compare their performance by implementing the same model on each simulator. Performance comparison is done using two performance metrics: effective simulation runtime and memory usage. In conclusion, the authors states that ns-3, OMNeT++ and JiST are all capable of carrying out large-scale network simulations. Overall, ns-3 demonstrated the best overall performance. A detailed comparison of network simulators was done in [18], which focused on the network simulators NS2, NS3, QualNet, GloMoSim, NetSim, OMNeT++, OPNET, TOSSIM, J-SIM, NCTUns, DRMSim, SSFNet, GrooveNet, and TraNS. The paper [18] contains information about the main features, advantages, limitations, supported

OS, hardware requirements etc. of all the above mentioned simulators, also it includes comparison tables listing license types, languages, GUI types, document availability, etc. Authors [13] analyze the accuracy of NS2 and the OPNET Modeler comparing the test bed results for CBR and FTP traffic with simulated results from ns-2 and OPNET Modeler, and concluding that significant effort was required to match the simulators with the test bed. In [14] the authors compared wireless network simulators (NS2, Qualnet, and OPNET) to a real testbed. The authors of [19] collate the results obtained from running NS2, Matlab, Opnet and Graphical Network Simulator-3 (GNS3) with the results obtained from a real network made up of Cisco routers. At first the authors [19] used a very simple network containing one IP routing device and measured the delay for single ICMP packets across the device, later they repeated the procedure in a more complex network similar to what can be found in a typical IP network. In order to compare the results from the simulations and real network results the authors [19] used Wireshark, and the results of OPNET were different from the real network results in the first scenario. It was not possible to run the second scenario because of the lack of parameters for traffic control. The results of the GNS3 simulation matched the results obtained from the Cisco network, and the authors [19] concluded that the only way of getting accurate simulation results about real networks is to use a mathematical model and implement it in Matlab or to create an application. In [20] the authors use datasets of actual attack traffic to create simulations in ns-2 simulator.

3. THE SIMULATOR CHOICE

According to the information in related works, there is no universal network simulator which can be used for creating any of the simulations. Each simulator has its advantages and disadvantages. That is why, it is very important to make a list of the research requirements when selecting a tool for simulation. Having studied the most commonly used network simulators we decided to use GNS3 simulator in our research. While using network simulators the researchers should compare the simulation results with the real network results. Comparing them we can see that many of the parameters (like application server settings), which can significantly affect the results, are missing in most of network simulators. This causes difficulties while comparing the simulated results with the real network results. In our previous work [16] we used Riverbed Opnet modeler for simulating a DDoS attack. Even if we were able to set traffic parameters, network links speed and server applications, more important parameters would be missing. That is why we've searched for an alternative. One of them is Graphical Network Simulator-3. The GNS3 is a free network software emulator first released in 2008. GNS3 provides a user friendly graphical interface displayed in Fig. 1, which allows us to create simulated topology without spending too much time.

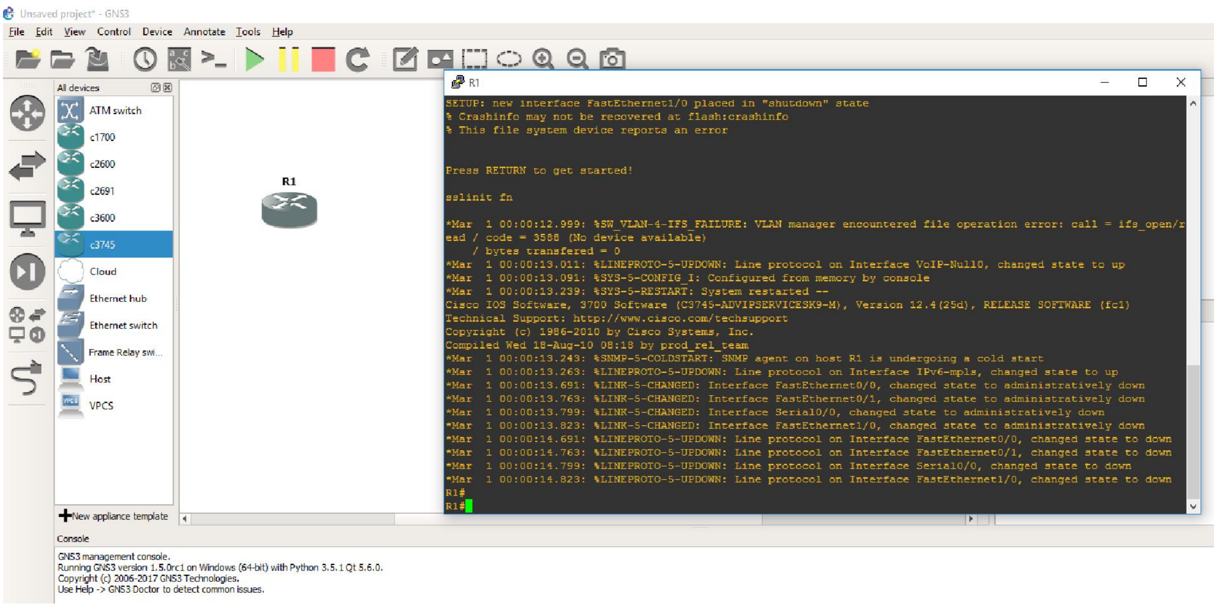

Fig. 1 – GNS3 GUI.

With GNS3 the combination of virtual and real devices can be made and used to simulate complex networks. It uses Dynamips emulation software to simulate Cisco IOS, it also supports devices from other network vendors like Juniper and others. If a network device IOS image is introduced into GNS3 then we may select allocated hardware resources, a number of network interfaces and their type. When the simulated device is added into the topology we can access it with a ssh remote control as it is shown in Fig. 1. One of GNS3 important advantages is the possibility to connect the simulated network topology to the real network environment. This can be done using the cloud virtual device from the device list in Fig. 1. We may select there a real or virtual network interface available on PC running GNS3. GNS3 is used by many large companies including Exxon, Walmart, AT&T and NASA, and is also popular while preparing for network professional certification exams.

4. THE SIMULATION

A model of computer network was created including a web server, 3 PCs of regular users and one attacker host. The network is served by Ethernet switches and Cisco routers. Then, we simulated a DOS attack from attacker host to see how it affects the work of web server and its accessibility for regular users. After that we try out some approaches for mitigating this attack. In Fig. 2 you can see what our topology looks like.

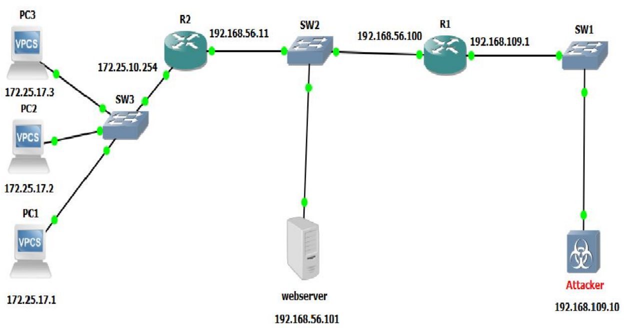

Fig. 2 – Simulated network topology.

In this topology the following devices are used:

1) The simulation host – OS: windows 10, CPU: core i5 6600 CPU, 16 GB RAM, HDD: 250 GB Samsung EVO 850;

2) Webserver – Fedora core 22 64 bit Linux system running apache 2.4.12 web server and mariadb 10.0.17 database server in default configuration. On the web server we have a default Wordpress 4.7 CMS installed. The web server OS is running in Oracle Virtual Box with 1 CPU core and 2 GB RAM;

3) Attacker – Kali Linux 4.6.0 OS running in virtual box with 1 CPU core and 2 GB RAM;

4) R1 and R2 routers are Cisco 3745 routers with 256 Mb RAM,

5) SW1,SW2,SW3 are GNS3 generic Ethernet switches;

6) PC1, PC2, PC3 are GNS3 Virtual PC Simulator.

All links in this simulation are set to 100Mbit/s speed. Virtual PC Simulator can be used to simulate end host in the network topology in Gns3 and run simple reachability tests like ping and traceroute. Though there are other alternatives available like Qemu and Virtual box, however, they are CPU intensive. Virtual PC Simulator is integrated with Windows and Linux machine and is very CPU light. GNS3 generic Ethernet switches are virtual devices created by GNS3 that do provide virtual connections between devices with much less resource usage compared to Cisco devices.

A. Scenario 1

Virtual PC Simulator allows making TCP ping by specifying destination port and protocol parameters. In the internal network we have 3 PCs which are in a separate LAN 172.25.10.0/24 and can access webserver through Cisco 3745 router. As it can be seen from Fig. 3, Fig. 4 and Fig. 5 we've launched tcp ping towards 3 on our PC's webserver to simulate regular users accessing web server.

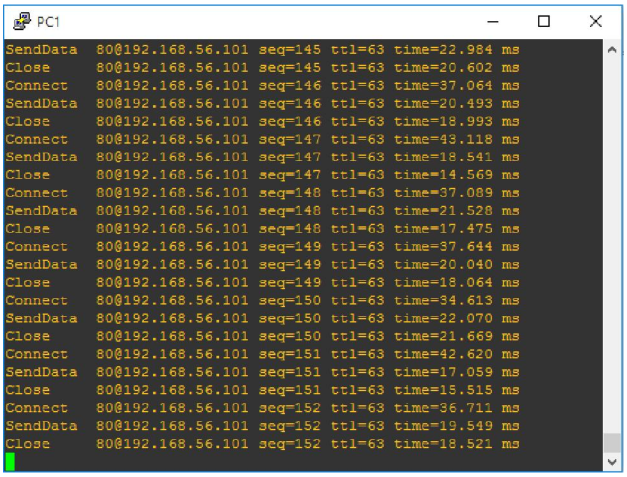

Fig. 3 – PC1 tcp ping towards web server before attack.

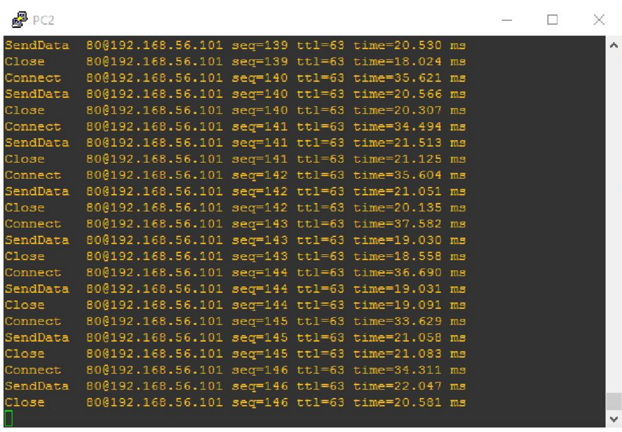

Fig. 4 – PC2 tcp ping towards web server before attack.

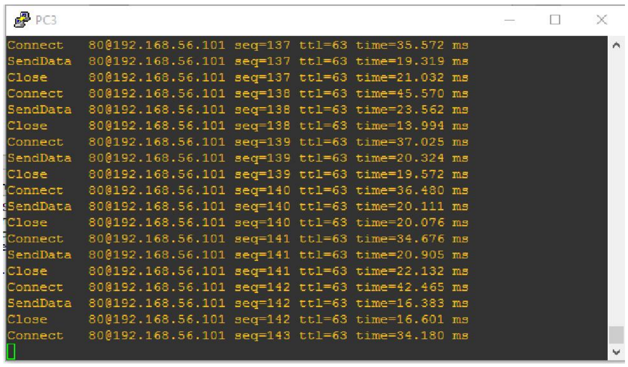

Fig. 5 – PC3 tcp ping towards web serve before attack.

At the next step we launch the attack from the attacker host which is in the outside network and can access webserver through Cisco 3745 router. For this simulation we don't use any Access Control List's or filtering rules on all of our routers, only the static routes between different networks are set. For the attack we use a simple perl script which creates multiple parallel connections to destination port 80 of our web server and prints the server's response. After launching attack we used Wireshark tool to examine the traffic which flows through the closest switch to the web server, this is shown in Fig. 6.

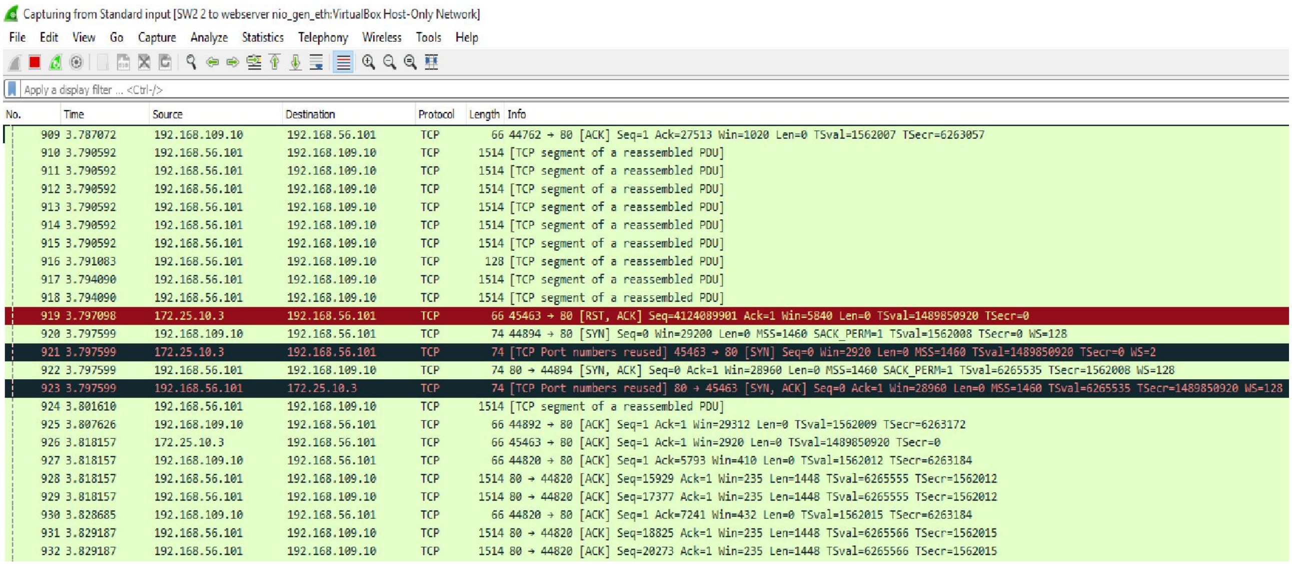

Fig. 6 – Webserver switch traffic flow statistics.

As we can see in Fig. 6 a large number of connections is generated by IP address 192.168.109.10 which is the attacker host and only few by 172.25.10.1 and 172.25.10.3 which are regular user hosts. Since the web server is running a default configuration, then after running the script multiple server instances are created and web server quickly goes out of memory and stops responding. Also since the server runs Wordpress CMS, it makes database connections on each page request, after launching the attack the maximum connection limit is overreached. In Fig. 7, Fig. 8, Fig. 9 we can see that ping statistics of legitimate users' hosts simulated by Virtual PC Simulator indicates that server stopped responding to users requests.

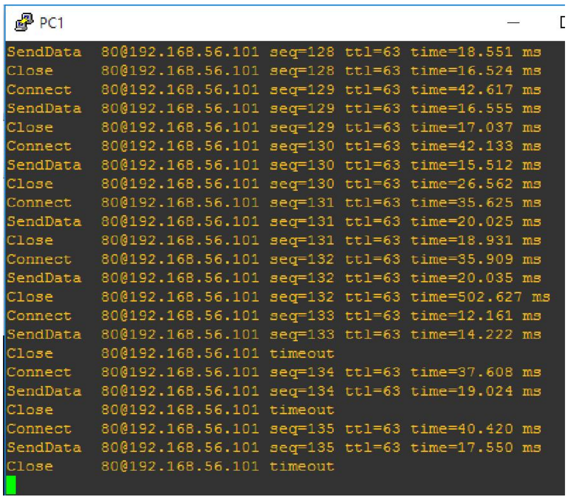

Fig. 7 – PC1 tcp ping towards web server during attack.

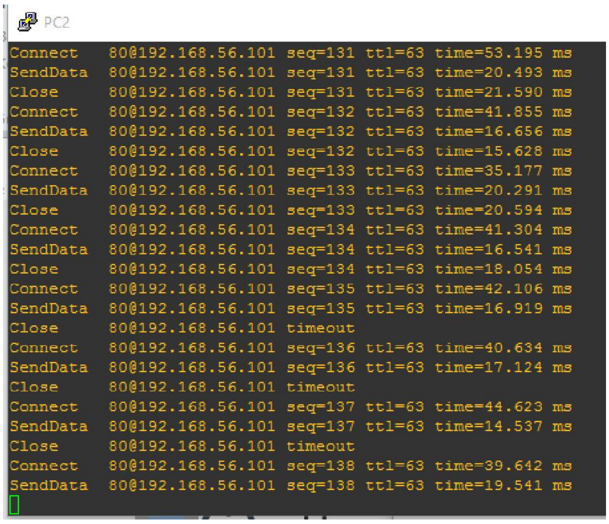

Fig. 8 – PC2 tcp ping towards web server during attack.

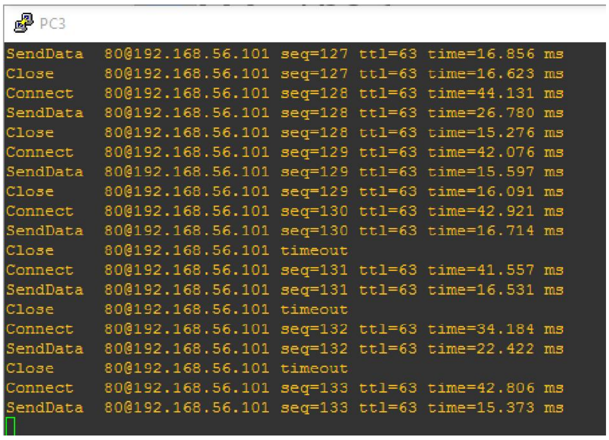

Fig. 9 – PC3 tcp ping towards web server during attack.

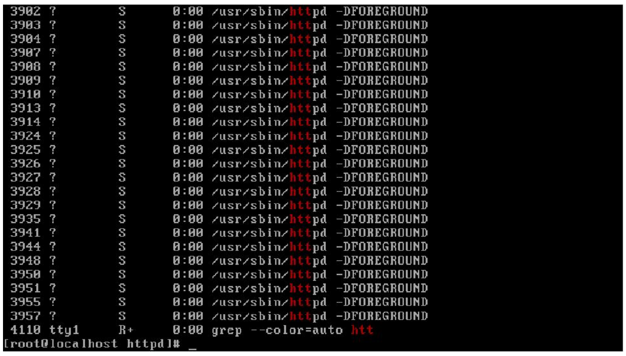

Fig. 10 – List of apache child processes when server is under attack.

In Fig. 10 we can see the list of apache child processes running on web server, at that time server stopped responding to legitimate users' requests.

B. Scenario 2

We installed the mod_evasive on the web server. It is an evasive maneuvers module for Apache that provides evasive action in the event of an HTTP DoS attack or brute force attack. It is also designed to be a detection and network management tool, and can be easily configured to talk to ipchains, firewalls, routers, and more. The mod_evasive presently reports abuse via email and syslog facilities. The mod_evasive enables to set the threshold for the number of requests for the same page (or URI) per page interval. Once the threshold for that interval has been exceeded, the IP address of the client will be added to the blocking list. Then we launch an attack again. As a result the attacking script, produced the output, is shown in Fig. 11.

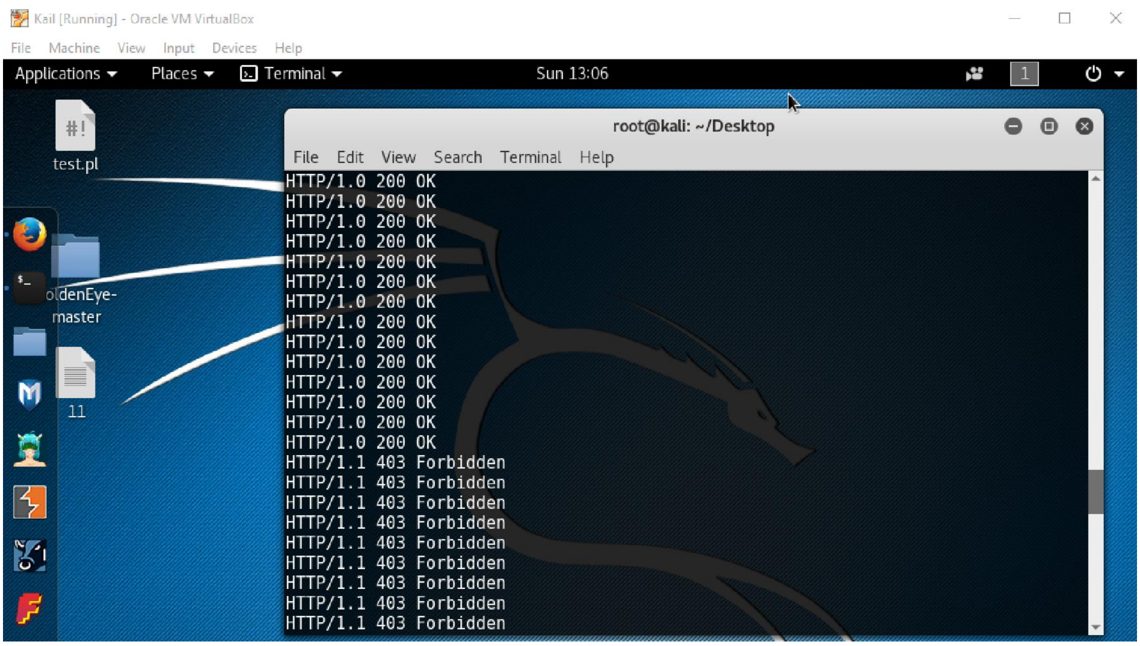

Fig. 11 – Attacking script output.

This means that after a short period of time an attacker IP was blacklisted by the web server. And instead of serving attacker's requests, the server started to respond with 403 Forbidden. This prevents server from making database connections, decreases server load and allows web server to be accessible for legitimate users.

5. CONCLUSION

In this paper we've shown some possibilities which GNS3 simulator can provide for scientists in the area of DoS and DDoS attacks simulation. The proposed simulation describes one of the DoS mitigation methods. However in real networks this method alone won't stand a chance against full scale DoS or DDoS attack. The aim of this simulation was not to present the best DDoS mitigation solution but to demonstrate a variety of parameters which can be simulated using GNS3. As we can see, such parameters as web server settings and defense modules settings can be used in GNS3 simulations. These parameters influence on performance of the server under attack and are unavailable in popular simulators like OPNET NS3 and others. GNS3 provides a very realistic approach to creation of the network simulations allowing setting a full variety of parameters which are available in the real computer networks. However, using of GNS3 compared to other network simulators has also some disadvantages. Because it employs hardware resources to simulate the work of all devices and a scalability is limited inside its topology. Another disadvantage is that GNS3 currently supports a limited amount of simulated hardware. Creation of more advanced simulations with the comparison of their results with real networks results should be a topic for the future studies.

6. REFERENCES

[1] M. Mazurek, P. Dymora, "Network anomaly detection based on the statistical selfsimilarity factor for HTTP protocol," *Przeglad elektrotechniczny*, Issue 1, pp. 127-130, 2014.

[2] T. Peng, C. Leckie, R. Kotagiri, "Proactively detecting DDoS attack using source IP address monitoring," in *Proceedings of the International Conference on Networking 2004,* Athens, Greece, May 9-14, 2004, pp. 771-783.

[3] M. Y. Su, G. J. Yu, C. Y. Lin, "A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach," *Communication Computers & Security*, Vol. 28, Issue 5, pp. 301-309, 2009.

[4] D. Mahajan, M. Sachdeva, "DDoS attack prevention and mitigation techniques," *International Journal of Computer Applications*, Vol. 67, Issue 19, pp. 21-24, 2013.

[5] S.R.S. Rao, *Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis*, The SANS Institute, Essex, 2011, 57 p.

[6] N. Z. Bawany, J. A. Shamsi, K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Arabian Journal for Science and Engineering*, Vol. 42, Issue 2, pp. 425-441, 2017.

[7] M. Sung, J. Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 14, Issue 9, pp. 861-872, 2003.

[8] X.-J. Wang, X.-Y. Wang, "Topology assisted deterministic packet marking for IP traceback," *The Journal of China Universities of Posts and Telecommunications*, Vol. 17, Issue 2, pp. 116-121, 2010.

[9] A. Balyk, U. Iatsykovska, M. Karpinski, Y. Khokhlachova, A. Shaikhanova, L. Korkishko, "A survey of modern IP traceback methodologies," in *Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, (IDAACS'2015),* Warsaw, Poland, September 24–26, 2015, Vol. 1, pp. 484-488.

[10] I. Kotenko, *Agent-Based Modelling and Simulation of Network Cyber-Attacks and Co-operative Defence Mechanisms*, in: Aitor Goti (Eds.), Discrete Event Simulations, Sciyo, Rijeka, 2010, pp. 223-246.

[11] S. Bezobrazov, A. Sachenko, M. Komar, V. Rubanau, "The methods of artificial intelligence for malicious applications detection in Android OS," *International Journal of Computing*, Vol. 15, Issue 3, pp. 184-190, 2016.

[12] I.V. Kotenko, A.A. Chechulin, "A cyber attack modeling and impact assessment framework," in *Proceedings of the 5th International Conference on Cyber Conflict 2013 (CyCon 2013),* Tallinn, Estonia, June 5, 2013, pp. 119-142.

[13] G. F. Lucio, M. Paredes-Farrera, E. Jammeh, M. Fleury, M. J. Reed, "OPNET-modeler and NS-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed," *in Proceedings of the 3rd WEAS International Conference on Simulation, Modelling and Optimization (ICOSMO 2003),* Singapore, December 5-7, 2003, Vol. 2, pp. 700-707.

[14] A. Rachedi, S. Lohier, S. Cherrier, I. Salhi, “Wireless network simulators relevance compared to a real testbed in outdoor and indoor environments,” *International Journal of Autonomous and Adaptive Communications Systems,* Vol. 55, Issue 1, pp. 88-101, 2012.

[15] A. Balyk, “A survey of the main approaches for DDoS attack simulation,” in *Proceedings of the 2016 International Conference Information Protection and Security of Information Systems,* Lviv, Ukraine, June 02-03, 2016, pp. 54-55. (in Ukrainian)

[16] A. Balyk, M. Karpinski “Using riverbed modeler for DDoS attack simulation,” in *Proceedings of the IV International Conference for students and PhD students engineer of XXI century*, Bielsko-Biala, Poland, December 02, 2016, pp. 53-58.

[17] E. Weingärtner, H. Vom Lehn, K. Wehrle, “A performance comparison of recent network simulators,” in *Proceedings of the 2009 IEEE International Conference on Communications*, Dresden, Germany, June 14-18, 2009, pp. 1287-1291.

[18] M. H. Kabir, S. Islam, J. Hossain, S. Hossain, “Detail comparison of network simulators,” *International Journal of Scientific & Engineering Research*, Vol. 5, Issue 10, pp. 203-218, 2014.

[19] J.N. Davies, P. Comerford, V. Grout, M.V. Verovko, S.S. Stasiuk, “Comparison of network simulators in IP networks,” *Journal Mathematical Machines and Systems*, Issue 4, pp. 3-11, 2014. (in Ukrainian)

[20] J. Singh, K. Kumar, M. Sachdeva, N. Sidhu, “DDoS attack’s simulation using legitimate and attack real data sets,” *International Journal of Scientific & Engineering Research*, Vol. 3, Issue 6, pp. 1-5, 2012.

Anatolii Balyk *graduated from the Ternopil Volodymyr Hnatiuk National Pedagogical University in 2009 obtaining the Master Degree in Informatics. He is working currently at Ternopil Ivan Puluj National Technical University.*

Research interests are: data communication and networking, programming.

Mikolaj Karpinski *graduated from the Lviv Polytechnic in 1980. He has been working in the University of Bielsko-Biala since 2002. Currently he is a professor and chairman of Department of Computer Science and Automatics. He obtains doctor’s and habilitation’s degrees in 1989 and 1996, respectively, and full professor’s title in Security of Information Technologies in 2001.*

His research interests are: cybersecurity, security of wireless networks, particular cryptographic methods of information defense, lighting engineering, electric and photometric measurements.

Artur Naglik *received Master’s degree in 2013 at University of Bielsko-Biala. Since 2011 he has been working at the University of Bielsko-Biala in Academic Center of Informatics.*

His research interests are wireless transmission and security.

PhD Gulmira Shangytbayeva *graduated from the Aktobe State University named after K.Zhubanov in 2004. She received Master’s degree in 2012. She defended her PhD doctoral thesis in 2015. She has been working in the Aktobe State University named after K. Zhubanov since 2004. Currently she is the head of the Computer Science Department.*

Her research interests are information security and computer systems.

Ihor Romanets *graduated from the Ternopil Academy of National Economy in 1997 (it’s a Ternopil National Economic University now). Currently he is a Director of Information Educational and Scientific Center at Ternopil National Economic University.*

His research interests are: cybersecurity, VoIP, wireless networks, video surveillance.