Analysis of Ping of Death DoS and DDoS Attacks

Fekadu Yihunie[1], Eman Abdelfattah[2], Ammar Odeh[3]
School of Computing[1,2], College of Applied Science[3]
Sacred Heart University[1,2], Al Maarefa Colleges for Science & Technology[3]
Fairfield, CT, USA[1,2], Riyadh, Kingdom of Saudi Arabia[3]
yihunief@sacredheart.edu[1] , abdelfattahe@sacredheart.edu[2], aoudah@mcst.edu.sa [3]

***Abstract*—Effects of ping of death attack from standalone and multiple attacking machines are compared with healthy network configuration by applying the attack to the Database and File Transfer Protocol (FTP) server. Riverbed Modeler Academic Edition 17.5 is used to design and analyze the performance of the network. A comparison of three scenarios is conducted. The first scenario is modeled with healthy and functional network topology. The second and third scenarios configured to attack the server from the standalone machine and multiple machines to simulate Denial of Service (DoS) attack and Distributed Denial of Service Attack (DDoS) respectively. The case studies are conducted based on the average response time, traffic received, traffic sent, upload and download response times. The DDoS attacks of the simulated network show dramatic declination of the performance and increase of the response time of the server.**

Keywords— Database, FTP, DoS, DDoS.

I. INTRODUCTION

Denial of Service (DoS) attack is one of the top exponentially growing types of cyber-attack, the most destructive and globally affecting business operations. By flooding the bandwidth or resources of a targeted machine or system, the attacker denies legitimate users from accessing the service. When the attacker uses a single machine to disrupt the service, it is known as DoS attack. The extended attack from DoS is distributed DoS (DDoS) which initiates the attack from multiple compromised devices to multiply the stress level of the attack on the targeted machine or system. The ultimate objective of both these attacks is crashing the service by overloading the network traffic to the system or by utilizing a huge amount of resources from the system. This paper presents one type of attacking technique called Ping of Death DoS and DDoS to evaluate its impact on the performance of the database and FTP server.

To avoid the complexity and unnecessary costs of building a physical network environment and to efficiently use the time, simulation software is ideal to experiment this kind of research [1]. As a result, this paper uses Riverbed Modeler Academic Edition to demonstrate two types of attacks on the Internet-based service [2]. Riverbed simulation software has a wide range of desirable configurations and performance analysis features in a virtual environment to simulate the network in different scenarios and produce analysis results.

This paper is organized as follows: Section II presents the related work, Section III, the designed network and three scenarios are presented, Section IV, illustrates and explains the results of the simulated network, and Section V offers the conclusion and future work.

II. RELATED WORK

The DoS and the DDoS attacks have a severe impact on computer networks. Researchers conduct intensive simulations to analyze the performance of their designed networks in the presence of these attacks and investigate how to mitigate against them.

Muraleedharan *et al.* propose a cross-layer security approach to detect denial of service (DoS) attacks to avoid collision attacks happening at the data link and network layers [3]. The proposed approach is suggested to achieve a high accuracy in predicting and defending the network against Denial of Service attack to other layers of the network, such as physical layer jamming attacks.

Rao implemented real-time networks to measure and analyze DoS attack by using network traffic monitoring tools [4]. Different mitigation strategies explained and enabled on Cisco routers to demonstrate the effectiveness of the mitigation plan in a small network topology. The author concluded that DoS attack has many ways of implementation and there is no single solution for all attacking techniques.

Ramanauskaite *et al.* proposed a composite denial of service attack model by combining bandwidth exhaustion, filtering and memory depletion to demonstrate real cyber-attack [5]. The experiment showed the main dependencies of the influence of attacker and victim's properties on the success probability of DoS attack. The composite DoS attack model has more accurate estimation of attack success probability than others DoS attack types.

Bonguet *et al*. discussed that DoS and DDoS attacks are serious threats to Cloud-based services availability because of numerous vulnerabilities introduced by the nature of cloud features like multi-tenancy and resource sharing [6]. The authors explored new types of XML and HTTP DoS attacks and explained the possible detection and mitigation techniques. The authors provided the existing defense products and evaluated them with the appropriate metrics and experimental design.

Cheung reviewed and analyzed the existing DoS threats against Domain Name System (DNS) service and proposed the countermeasures to these threats [7]. Although the existing and proposed countermeasures appear to be useful. The author suggested that conducting a comprehensive analysis on the countermeasures and improved understanding of the effectiveness and limitations derive accurate security values in the attack tree.

Taghavi *et al*. explored the scope of the DDoS flooding attack problem and suggested a solution by categorizing the attacks [8]. The authors highlighted the need for a comprehensive distributed and collaborative defense approach to mitigate the DDoS flooding attacks. The authors suggested that more nodes should be involved in detecting, preventing, and responding to DDoS flooding attacks to implement hybrid and distributed defenses.

Joodat *et al*. investigated the present state of Internet of Things (IoT) and explained the impact of IoT devices in DDoS attacks. The authors mentioned more secure authentication practices for IoT devices to reduce botnet attacks [9]. Furthermore, they recommended that manufacturers of IoT devices implement virtual patching feature on software updates to minimize the risk of zero-day attacks.

III. Designed Network

The network topology of the three scenarios: Healthy network topology, DoS attacked network topology, and DDoS attacked network topology are shown in Figures 1, 2 and 3, respectively. The Ping Parameters Configurations are shown in Figure 4.

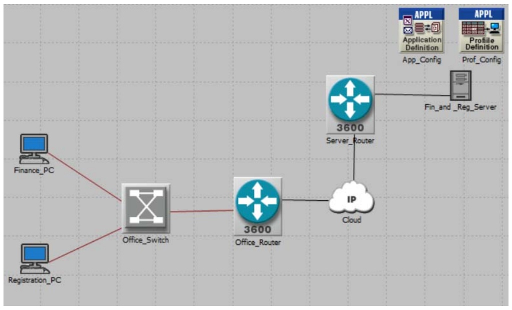


Figure 1. Network Topology for Healthy Network

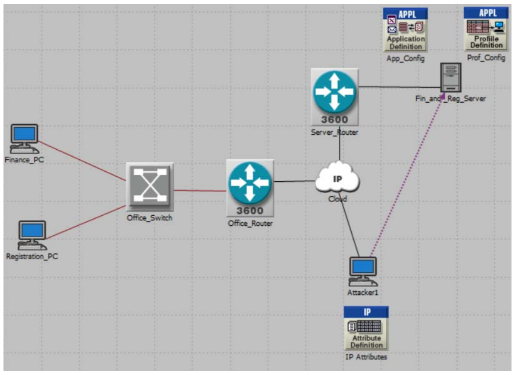


Figure 2. Network Topology for DoS attack

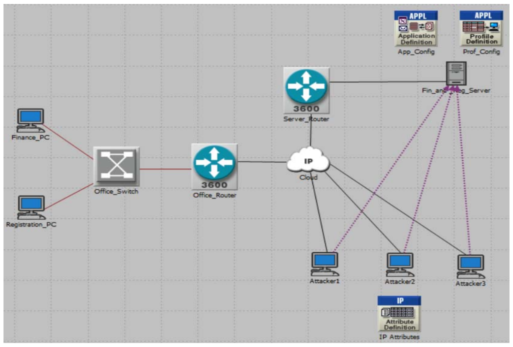
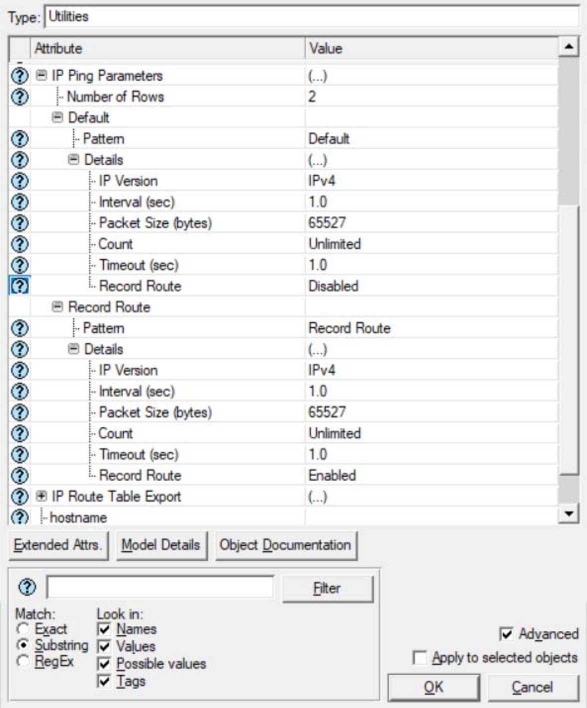


Figure 3. Network Topology for DDoS attack



Type: Utilities

Attribute	Value
⊟ IP Ping Parameters	(...)
Number of Rows	2
⊟ Default	
Pattern	Default
⊟ Details	(...)
IP Version	IPv4
Interval (sec)	1.0
Packet Size (bytes)	65527
Count	Unlimited
Timeout (sec)	1.0
Record Route	Disabled
⊟ Record Route	
Pattern	Record Route
⊟ Details	(...)
IP Version	IPv4
Interval (sec)	1.0
Packet Size (bytes)	65527
Count	Unlimited
Timeout (sec)	1.0
Record Route	Enabled
⊞ IP Route Table Export	(...)
hostname	

Match: ○ Exact ● Substring ○ RegEx

Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

☑ Advanced

□ Apply to selected objects

Figure 4. the Ping Parameters Configurations

The first scenario shows a healthy and functional network that is used as a benchmark to compare with the second and third scenarios with respect to the response time. All scenarios are configured as an office network with two departments; Finance and Registrar that are connected remotely over the Internet to a Database and FTP server. Two workstations, one switch and one Cisco router are used in the office network. The database and FTP server is hosted somewhere outside of the office network. It is connected to Cisco router and provide the service over the Internet to the client workstations.

In the first scenario, the server application definitions configured in two rows. The first is a registrar database with a capacity of handling high load requests, and the second is Finance FTP server with capacity of handling high load FTP requests. The server's profile configured in two rows: the registrar application as REG profile and the finance FTP server as FIN profile. The two profiles are assigned to application-supported profiles of Registration-PC and Finance-PC respectively.

The second scenario duplicated from the first scenario with some additional configurations. Standalone attacking machine added to the network topology by using IP ping traffic link to the server by assigning source and destination addresses of the attack. In the attribute definition of IP ping parameters, two rows are configured with packet size 65,527 bytes, close to the maximum allowed packet size in IPv4, unlimited count, and one second timeout interval.

The third scenario duplicated from the second scenario with additional two attacking machines to multiply the pressure of the ping request attack on the server. The additional attacking machines connected to the server by using IP ping traffic link that is configured with the appropriate source and destination addresses.

The simulation configured for a duration of 5 hours with 100 values per statistic to capture the performance measurements of the Database server; DB Query Response Time (sec), Traffic Received (bytes/sec), and Traffic Sent (bytes/sec). Moreover, Download Response Time (sec), Traffic Received (bytes/sec), Traffic Sent (bytes/sec) and upload Response Time (sec) measured for the FTP server.

IV. Performance Evaluation

Figure 5 shows Database Query Response Time that is the time elapsed between sending a request by Database Query Application (workstation) and receiving the response from the Database Server [10]. All response packets sent from a server to a Database Query application are collected. Database Query Response Time, in the case of healthy network and DoS attacked network scenarios, overlap. However, the negative impact on Database Query Response Time in case of DDoS attacks is measured up to 2000 seconds. The attacked server stopped responding after 45 minutes because of the severe impact of the DDoS attack on that server. This clearly demonstrates the impact of DDoS attacks on Internet-based services.

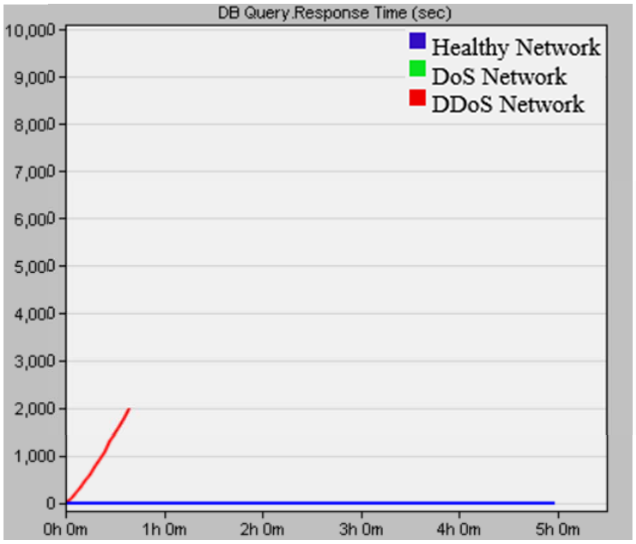


Figure 5. Database Query Response Time

Figure 6 shows average Traffic Received in bytes per second to all Database Query Applications (workstations) by the transport layers in the network. Both in the healthy network and DoS attacked network scenarios the traffic received in bytes per second are comparable. However, in case of the DDoS attacked network, the received traffic deteriorated gradually and then stopped completely close to 3 hours of server operation.

Figure 7 shows the average Traffic sent in bytes per second to the transport layers by all Database Query Applications (workstations) in the network. Both in the healthy network and DoS attacked network, traffic sent in bytes per second are comparable. However, in the DDoS attacked network the traffic sent declined gradually and stopped before 3 hours of server operation.

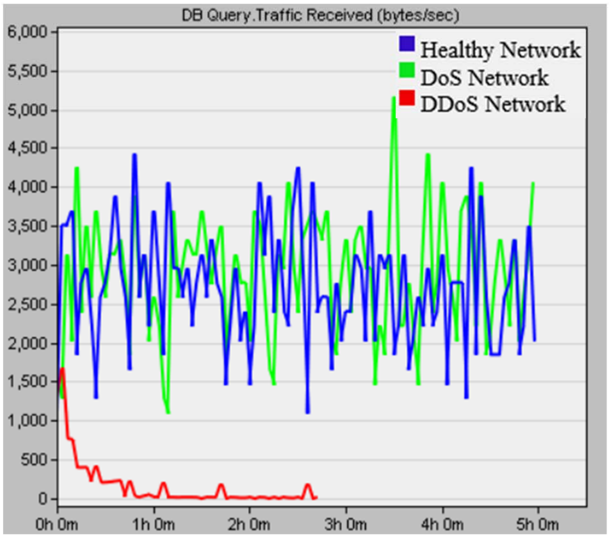


Figure 6. Database Traffic Received

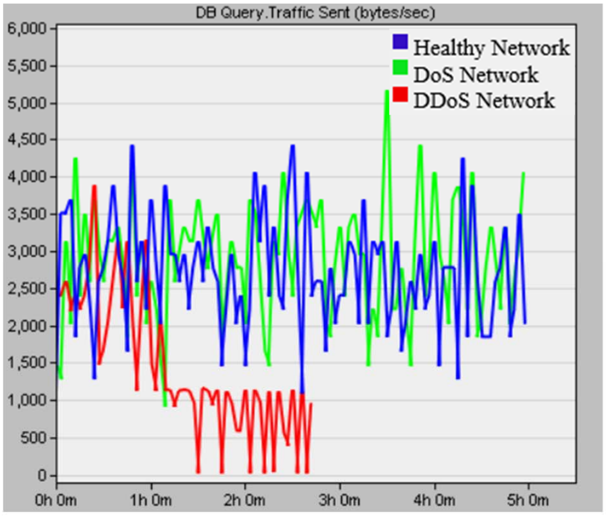


Figure 7. Database Traffic Sent

Figure 8 shows the average Upload Response Time between sending a request for a file and receiving the response from FTP server to an FTP application (workstation). FTP Server response time in case of healthy network and DoS attacked network scenarios overlap. However, the negative impact on FTP server average response time in DDoS attacks is observed up to 250 seconds. Then, the attacked server stopped responding completely around 3 hours of simulation indicating the severe impact of the DDoS attack on that server.

Figure 9 shows the average Traffic Received in bytes per second to all FTP Applications (workstations) by the transport layers in the network. Both in the healthy network and DoS attacked network scenarios, the traffic received in bytes per second are comparable. However, in case of DDoS attacked network the traffic received from the FTP server deteriorated gradually before stopping completely around 3 hours of simulation.

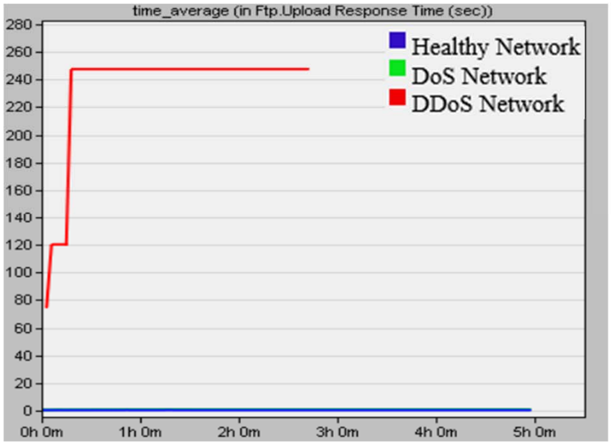


Figure 8. FTP upload response time

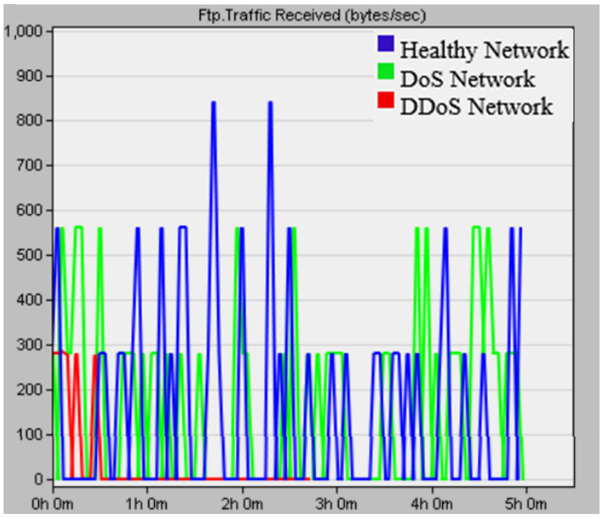


Figure 9. FTP Traffic Received

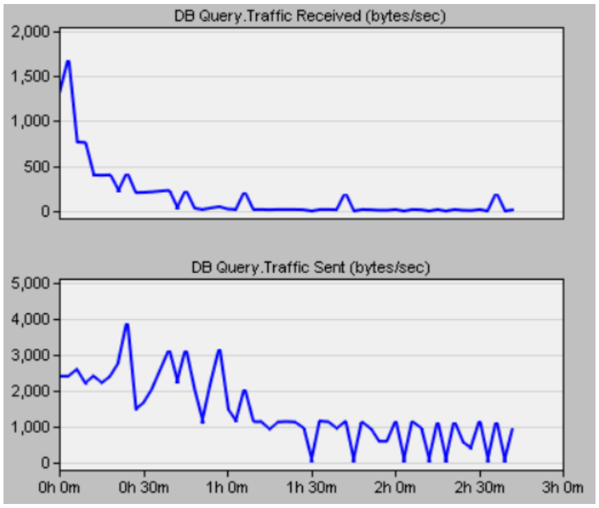


Figure 10. DDoS: DB Query Traffic Received and Sent

Figure 10 shows the DB Query Traffic Received and Traffic Sent in case of DDoS. The significant difference between Traffic Received and Traffic Sent is demonstrated.

V. Conclusion

The performance of the simulated network evaluated in three different scenarios that clearly showed how the DDoS attacks affect the smooth operation of Internet-based services. By analyzing standalone and multiple machine attacks, the negative impact of the DoS and the DDoS attacks is examined. This paper demonstrates how the DDoS attacks disrupt the smooth business operation of the organization and how the DoS attacks affect the productivity of the business.

Since 1988, DoS attacks were one of the common threats to the computing industry [9]. Businesses operation disrupted, and poor service resulted due to the attacks. Internet Service Providers (ISPs) and public Domain Name System (DNS) servers were affected severely by these attacks.

Security software, hardware vendors and security researchers should consider and work together to prevent new ways of DDoS attacks in the future that may impact the global network infrastructure, governmental organizations, corporate businesses, and individuals. Collective measures of protection will minimize the impact and reduce the magnitude of the attack. Security administrators should monitor their networks actively to mitigate the threats of the attack and protect networked devices not to be part of the botnet for the use of other attacks. In our future work, we plan to integrate and analyze different countermeasures to mitigate both DoS and DDoS attacks.

VI. References

[1] Jinhua Guo, Weidong Xiang, Shengquan Wang, “Reinforce Networking Theory with OPNET Simulation,” University of Michigan-Dearborn, MI, USA.

[2] Riverbed Modeler. http://www.riverbed.com/

[3] Rajani Muraleedharan, Lisa Ann Osadciw, “Cross Layer Denial of Service attacks in Wireless Sensor Network Using Swarm Intelligence,” 40th Annual Conference on Information Sciences and Systems, Princeton University, IEEE 2006.

[4] Subramani Rao Sridhar Rao, “Denial of Service attacks and mitigation techniques,” Real time implementation with detailed analysis, SANS Institute, 2011

[5] Simona Ramanauskaite, Antanas Cenys, “Composite DoS Attack Model,” ISSN 2029-2341 print / ISSN 2029-2252 online. 2012.

[6] Anrien Bonguet, Martine Bellaiche, “A survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing,” Computer Engineering and Engineering Software, École Polytechnique de Montréal, QC H3T 1J4, Canada, 2017.

[7] Steven Cheung, “Denial of Service against the Domain Name System: Threats and Countermeasures,” SRI International, July 27, 2005.

[8] Saman Taghavi, James Joshi, David Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” IEEE Communications Surveys and Tutorials.

[9] Robert Joodat, Eric Wang, “Distributed Denial of Service (DDoS) Attacks and IoT Security,” Technical Report, https://www.grin.com/document/371086

[10] Adair, John G., Richard A. Demers, Dusan Ecimovic, Robert J. Grafe, Robert D. Jackson, Bruce G. Lindsay, Michael E. Murphy et al. "Query language execution on heterogeneous database servers using a bind-file bridge between application and database languages." U.S. Patent 5,257,366, issued October 26, 1993