PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

MOHAMED BOUDIAF UNIVERSITY - M'SILA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

COMPUTER SCIENCE DEPARTMENT

DISSERTATION

Submitted in partial fulfillment of the requirements for the Degree of MASTER

Domain: Mathematics and Computer Science
Branch: Computer Science
Specialty: Networks

By: AICHAOUI TARIQ

TOPIC

Framework for detecting DoS/DDoS Attacks against Web servers

Publicly defended: / /2016 before a Jury composed of :

Ms. SAOUDI LALIA	**University of M'sila**	**Supervisor**
.....	**University of M'sila**	**Chair**
.....	**University of M'sila**	**Examiner**
.....	**University of M'sila**	**Examiner**

Academic Year: 2015 /2016

TABLE OF CONTENTS

1 Context:

Web applications are becoming more popular and widely being used in all aspects of work and social activities, unfortunately, with the growth of web technologies and availability of resources over internet number of attacks on servers providing these services, resources are increased.

One of the most popular attack targets are web-servers and web-based applications. A web server is a program that serves a request using the HTTP protocol. Initially web servers were using static Hyper Text Markup Language (HTML) pages to provide information. But nowadays the web servers provide dynamic services using database queries, executable script,etc. for providing information. The web is used for different kinds of services and various applications such as emailing,banking applications, real-time communication, etc.

2 Statement of the Problem:

Denial of service (DoS) attack against web server is one of the most dangerous attacks. Which attempts to make the web server unavailable to serve up the web sites they host to legitimate visitors. Usually, the users of web-servers request and send information using queries, which in HTTP traffic are strings containing a set of parameters having some values. Attackers are able to manipulate these queries and create requests which can corrupt the server.

Denial of Service attacks can result in significant loss of service, money and reputation for organizations. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. An HTTP Denial of Service attack can also destroy programming and files in affected computer systems. In some cases, HTTP DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

3 Objectives:

3.1 General Objectives

In this work, we propose an anomaly based system developed to detect DoS/DDoS attacks against web servers. The detection focus on two most attack target protocols TCP and HTTP.

3.1 Specific Objectives

The design of the framework handles all aspects of HTTP and TCP based DDoS attacks through the following three subsequent framework's layers:

- Firstly, an outer detector blocks attacking IP source if it is listed on the black list table.
- Secondly, the IP spoofed detector to validate whether the incoming request is launched by true IP source or a spoofed IP.
- Thirdly, two classifier modules are proposed to detect HTTP/TCP DDoS attacks, for this modules we have to :
    - Select the relevant features of the HTTP protocol, to calculate a new set of features to classify the HTTP traffic as normal or DoS attack.
    - Select the relevant features of the TCP protocol, to calculate a new set of features, to classify the TCP traffic as normal or DoS attack.

4 Thesis Outline:

To meet our objective this thesis is structured as follows:

The First chapter considers the content of our work. Firstly, we provide an overview of Hypertext Transfer Protocol and how HTTP client and server communicate, then we introduce the denial of service attack, its different concepts, techniques and tools.

The second chapter provide an overview of intrusion detection systems and taxonomy of defense mechanisms against DoS/DDoS attacks.

The third chapter presents the conceptual aspect of our DoS/DDoS attack detection framework and its different components, which are a packet sniffer, IP spoofing detector and TCP/HTTP classifier modules.

The fourth chapter shows the experiments to demonstrate the effectiveness of our proposed framework.

Finally, we conclude this thesis by a general conclusion, recommendations and different perspectives.

Undoubtedly, DDoS attacks present a serious problem in the Internet and challenge its rate of growth and wide acceptance by the general public, skeptical government and businesses. As the use of internet increasing, the need for more efficient DDoS detection system becomes critical.

The great complexity of the DoS/DDoS problem suggests that its solution will require the use of multiple defenses .Our implemented framework proposes an alternative solution which work on collaborative, multilayers manner to detect HTTP and TCP based DoS/DDoS attacks. This solution starts by a simple traffic filter, which detect the black listed IP source, then pass to the second medium filter to detect the IPs spoofed, finally the traffic pass into two parallel filters: TCP filter and HTTP filter, for each detected anomaly, the traffic will be blocked.

In this work, we collected a new dataset that includes modern types of DoS/DDoS attack, which were not been used in previous researchs. The collected data has been recorded for different types of attack that target the Application and transport layers. Random Tree classifier algorithm was applied on the collected dataset to classify the normal traffic and DDoS types of attack namely: SlowPost, Slowloris, HOIC, LOIC-HTTP, LOIC-TCP, SynFlood.

To evaluate our DoS/DDoS framework we split our dataset into four type of traffic, which are HTTP-Normal, TCP-Normal, HTTP-DDoS and TCP-DDoS traffics. The both of TCP-Normal and TCP-DDoS traffics are used to test the performance of TCP classifier. Simultaneously, HTTP -Normal and HTTP-DDoS traffics are used to test the performance of TCP and HTTP classifiers. The evaluation proves that the proposed method can successfully identify DDoS attacks with very high detection rates.

As perspective we propose to integrate our framework with snort IDS to generate snort rules for each reported anomaly.

Bibliography

[01] R. Fielding, J. Gettys , J. Mogul , H. Frystyk, and T. Berners-Lee, "Hypertext Transfer Protocol --HTTP/1.1", RFC 2616, June 1999.

[02] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition, John Wiley & Sons, Inc, Indianapolis, Indiana , October 2011.

[03] HTTP tutorial, http://www.tutorialspoint.com/http/http_pdf_version.htm ,visited 24/12/2015.

[04] Programming notes , HTTP (HyperText Transfer Protocol), https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/HTTP_Basics.html - visited 29/01/2016 .

[05] Applicure , Prevent Denial of Service (DoS) Attacks , http://www.applicure.com/solutions/prevent-denial-of-service-attacks , visited – 01-02-2016.

[06] L. Stein, J. Stewart , The World Wide Web Security FAQ , https://www.w3.org/Security/faq/wwwsf6.html - visited 04/02/2016.

[07] M. ABLIZ , Internet Denial of Service Attacks and Defense Mechanisms, Department of Computer Science, University of Pittsburgh, 2011.

[08] CERT , Denial of Service Attacks , 1997 https://www.cert.org/information-for/denial_of_service.cfm? -visited 06/02/2016

[09] Anne Carasik-Henmi, W. Shinder, Dr. Thomas, Robert J. Shimonski , Debra Littlejohn , Best Damn Firewall Book Period , Syngress ,2011 .

[10] Cisco, A Cisco Guide to Defending Against Distributed Denial of Service Attacks , http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html -visited 06/02/2016

[11] Jema D. Ndibwile, A. Govardhan , K. Okada, Y. Kadobayashi , Web Server Protection against Application Layer DDoS Attacks using Machine Learning and Traffic Authentication , IEEE 39th Annual International Computers, Software & Applications Conference , vol: 3, 2015, pp. 261-267.

[12] Gulshan Kumar , Understanding Denial of Service (Dos) Attacks Using OSI Reference Model , International Journal of Education and Science Research, vol: 1, 2004, pp. 10-17.

[13] Mohammed A. Saleh , Azizah A. Manaf , A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks , The Scientific World Journal,vol:2015 ,2015.

[14] M. Aiello, E. Cambiaso, M. Mongelli, G. Papaleo , An On-Line Intrusion Detection Approach to Identify Low-Rate DoS Attacks , 2014 International Carnahan Conference on. IEEE, 2014, pp. 1-6.

[15] A. Pras, A. Sperotto, Giovane C. M. Moura,I. Drago, R. Barbosa, R. Sadre,R. Schmidt and R. Hofstede , Attacks by "Anonymous" WikiLeaks Proponents not Anonymous , 2010.

[16] Check Point Whitepaper , DoS Attacks: Response Planning and Mitigation , August 2012

[17] Sean Gallagher , High Orbits and Slowlorises: understanding the Anonymous attack tools, Feb 16, 2012 , http://arstechnica.com/business/2012/02/high-orbits-and-slowlorises-understanding-the-anonymous-attack-tools/2/ - visited 10/02/2016.

[18] Imperva , Hacker Intelligence Initiative, Monthly Trend Report #12, September 2012.

[19] Impreva, https://www.incapsula.com/ddos/attack-glossary/http-flood.html, visited 16/02/2016.

[20] Verma Nischal, Francois Trousset, Pascal Poncelet, Florent Masseglia. Intrusion Detections in Collaborative Organizations by Preserving Privacy, Advances in Knowledge Discovery and Management,volume: 292, 2010, pp. 235-247.

[21] Chadouli Youssouf, Saoudi Lalia, "A New Feature Selection approach For Network Intrusion Detection Systems", Master thesis, University of Msila , 2014.

[22] Nicholas J.Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee, Ronald A.Olsson . A Methodology for Testing Intrusion Detection Systems, IEEE Transactions on Software Engineering, volume:22, 1996,pp 719-729.

[23] Rebecca Bace, Peter Mell. Intrusion Detection Systems, National Institute of Standards and Technology,2001.

[24] Rafeeq Ur Rehman ,Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, Upper Saddle River, NJ : Prentice Hall PTR, 2003.

[25] Herv´e Debar, An Introduction to Intrusion-Detection Systems, Proceedings of Connect, volume :2000, 2000.

[26] Michael Sweeney, C. Tate Baumrucker , James. D. Burton, Ido Dubrawsky, Cisco Security Professional's Guide to Secure Intrusion Detection Systems, 2003.

[27] Jacob .B, Automatic XSS detection and Snort signatures/ACLs generation by the means of a cloud-based honeypot system ,Doctoral dissertation, Edinburgh Napier University,2011.

[28] D.E. Denning, An Intrusion-Detection Model, IEEE Trans. Software Eng, volume:13, 1987, pp. 222-232.

[29] Jelena Mirkovic, Gregory Prier, Peter Reiher, Attacking DDoS at the Source, Network Protocols 10th IEEE International Conference, vol: 2002.pp. 312-321

[30] Christos Douligeris , Aikaterini Mitrokotsa , DDoS attacks and defense mechanisms: classification and state-of-the-art , Computer Networks, vol:44, October 2004,pp. 643-666.

[31] Saman Taghavi Zargar, James Joshi and David Tipper, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS,Vol:15, 2013, pp. 2046-2069.

[32] Thomer M.Gil ,Massimiliano Poletto , MULTOPS: a data-structure for bandwidth attack detection, 10th USENIX Security,2001,pp 23-38.

[33] Rajkumar , ManishaJitendra Nene , A Survey on Latest DoS Attacks:Classification and Defense Mechanisms , International Journal of Innovative Research in Computer and Communication Engineering , vol :1,October 2013.

[34] Steven M. Bellovin ,ICMP Traceback Messages, AT&T Labs Research, Florham Park,2003.

[35] Puneet Zaroo , A Survey of DDoS attacks and some DDoS defense mechanisms , Advanced Information Assurance (CS 626), 2002.

[36] Haining Wang, Danlu Zhang, Kang G. Shin, Detecting SYN Flooding Attacks, Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol: 3 ,2002,pp 1530-1539.

[37] W. Eddy, TCP SYN Flooding Attacks and Common Mitigations, RFC 4987 , August 2007.

[38] Cheng Jin, Haining Wang, Kang G. Shin, Hop-Count Filtering: An Effective Defense Against Spoofed Traffic , 10th ACM conference on Computer and communications security ,2003,pp 30-41.

[39] Naga Shalini Vadlamani , A Survey on Detection and Defense of Application Layer DDoS Attacks , Master Thesis - Science in Computer Science,*University of Nevada, Las Vegas*, December 2013.

[40] Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, Raman K. Mehra , Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables -A Feasibility Study , IEEE/IFIP International Symposium ,2001,pp. 609-622.

[41] Dileep Kumar G,CV Guru Rao,Manoj Kumar Singh,Farid Ahmad, Using Jpcap API to Monitor, Analyse and Report Network Traffic for DDoS Attacks , 14th International Conference on Computational Science and Its Applications , 2014.

[42] Opeyemi.A. Osanaiye, Short Paper: IP Spoofing Detection for Preventing DDoS Attack in Cloud Computing , International Conference on Intelligence in Next Generation Networks,2015,pp 139-141.

[43] Steven J. Templeton, Karl E. Levitt , Detecting Spoofed Packets, DARPA Information Survivability Conference and Exposition, vol:1, 2003, pp. 164-175.

[44] Hanaa A. Qeshta , Tawfiq S. Barhoom, Adaptive Worms Detection Model Based on Multi Classifiers , Thesis on Master of Science In Information Technology , Islamic University – Gaza ,2012.

[45] R Vijayasarathy , Balaraman Ravindran, S V Raghavann, A System Approach to Network Modeling for DDoS Detection using a Naive Bayesian Classifier , Third International Conference on Communication Systems and Networks ,2011,pp. 1-10.

[46] V.Mohan Patro, Manas Ranjan Patra , Augmenting weighted average with confusion matrix to enhance classification accuracy, ransactions on Machine Learning and Artificial Intelligence, vol:2, 2014,pp. 77-91.

ملخص: أصبحت العديد من المواقع الإلكترونية في وقتنا الحالي تواجه خطر ما يسمي بهجمات الحرمان من الخدمة. هاته الهجمات تظهر عندما يحاول المهاجم جعل موارد خادم الويب غير متاحة لمستخدميها مما يؤدي الى توقف الموقع عن العمل .وبالرغم من جهود العديد من الباحثين الى أنه لا يوجد حل أمثل للتصدي لجميع أنواع هجمات حجب الخدمة.

لذلك اقترحنا نظام مبتكر يعمل على كشف كل أنواع هجومات الحرمان من الخدمة التي تقوم على مبدأ استغلال البرتوكول TCP والبرتوكول HTTP. وذلك اعتمادًا على ثلاث طبقات من الكشف:

- أولاً، كاشف خارجي يوقف جميع التدفقات الشبكية القادمة من مصدر هو ينتمي أصلا الى القائمة السوداء الممنوعة من التواصل مع الخادم.
- ثانياً، كاشف للعناوين (IP) ذات المصدر المغشوش.
- ثالثاً، مصنِفين مقترحين لكشف هجمات الحرمان من الخدمة التي تعتمد على البرتوكولين HTTP وTCP. ولتصميم هذين المصنِفين قمنا بما يلي:
  - انتقاء اهم حقول البرتوكولHTTP، وذلك لحساب واستنتاج الخصائص التي تسمح لنا بتصنيف تدفق HTTP العادي وتدفق HTTP الخاص بهجمات الحرمان من الخدمة.
  - انتقاء اهم حقول البرتوكولTCP، وذلك لحساب واستنتاج الخصائص التي تسمح لنا بتصنيف تدفق TCP العادي والتدفقTCP الخاص بهجمات الحرمان من الخدمة.

الكلمات المفتاحية: الكشف عن هجوم الحرمان من الخدمة، خادم الويب، نظام الكشف عن التسلل، شجرة القرارات، كشف عنوان IP مغشوش.

Abstract: Recently many prominent web sites face so called Denial of Service Attacks (DoS).these attacks occur when an attacker attempts to make the web server, or servers, unavailable to serve up the web sites they host to legitimate visitors. Despite many researchers' efforts, no optimal solution that addresses all sorts of DoS/DDoS attacks is on offer.

Therefore, our framework aims to propose an alternative solution which handles all aspects of HTTP and TCP based DDoS attacks through the following three subsequent framework's layers:

- Firstly, an outer detector blocks attacking IP source if it is listed on the black list.
- Secondly, the IP spoofed detector to validate the source of incoming requests.
- Thirdly, two classifier modules are proposed to detect HTTP/TCP DDoS attacks, for this modules we :
  - Select the relevant features of the HTTP protocol, to calculate a new set of features to classify the HTTP traffic as normal or DoS attack.
  - Select the relevant features of the TCP protocol, to calculate a new set of features, to classify the TCP traffic as normal or DoS attack.

Keywords: Denial of service attack (DoS) detection, Web server attack, Intrusion detection system, Decision tree, IP spoofed detection.