ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Detecting Client Based HTTP Attacks on Proxy Server by XSS Attack & SQL Injection

Komal Patole [1]

P.G. Student, Department of Computer Engineering, SKNCOE Engineering College, Vadgaon, Pune, India[1]

ABSTRACT: Today, peoples use large amount of workstation particularly for internet submission. Most of people do their transaction through internet use, so most of chances of personal blogs, accounts gets hacked then need to be provide more refuse for both web server and database server. To avoid this problem, Http attack system is used. The http attack system is used to identify and allow attack using IDS(Intrusion detection system). Http attacks prevents attacks user account from intruder from hacking users account. By using Intrusion detection system is a system can supply security for both web server and database server using map of demand and query. An IDS (intrusion detection system) that model the network actions of user sessions across together the front-end web server and back-end database.

KEYWORDS: Security economics, web proxy, data extraction, distributed denial of service attack, XSS attack

I. INTRODUCTION

Now a day computers are widely used for web application. Majority of transactions are done online these days. Thus data from web server and database server are given to be hacked easily which relies to provide more security to web applications. To avoid this problems Http attack system is used.

Distributed Denial-Of-service

In given networks, network application and web application are growing quickly, as the internet is an entire part of the modern world. Most business and other applications are provided through the internet. According to the network security experts all problems are related to availability, integrity and confidentiality. Most of the attacks are created in application layers. Figure shows the architecture of the DDoS attack. In this architecture HTTP based attacks is used, its identifying malicious code in the incoming HTTP request and removes bad request before they are proposed. Zombie is a second layer of DDoS attack, it is a program which secretly takes over another networked computer then uses it to indirectly launch attacks. In OSI layer some attacks are possible is as follows, HTTP/HTTPS POST flood, HTTP/HTTPS GET Flood, Cross Site Scripting (CSS), SQL Injection, Proxy based HTTP attacks, Identify Spoofing.

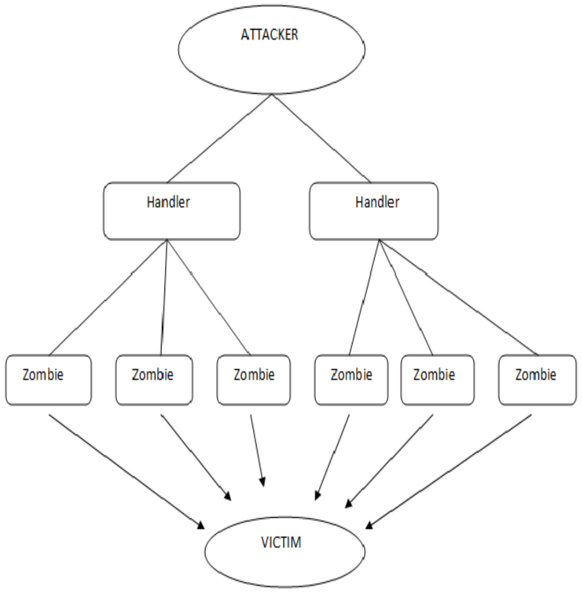

Figure 1. Architecture of DDoS attack

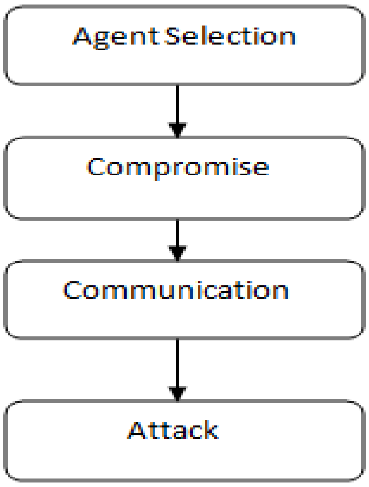

Figure 2. DDoS attack process

Classification of DOS attack:
Application level floods: An application-level flood attack is when an attacker exploits bugs in any sort of networked application, such as buffer overflows, in order to execute a DoS attack.
Smurf Attack: The Smurf attack is a type of distributed denial-of-service attack in which a system is shaft with spoofed ping messages. This creates network traffic on the victims network. Smurf takes well-known facts about internet

protocols internet control message protocol (ICMP) into account. ICMP is used by network administrators to exchange information about network also used to ping other nodes to determined to their operational status.

SYN flood: This is another type of denial-of-service attack. It is a normal connection between then user and server. The three-way handshake is correctly performed. The attacker sends several packets but does not send the ACK back to the server.

Teardrop attacks: teardrop attack is a DoS attack that involves sending fragmented packets to a target. Since the machine receiving such packets cannot correspond to them due to a bug in TCP/IP fragmentation reassembly the packets simultaneity one another, crashing the target network device. This happens on older operating systems such as windows 3.1x, windows 95, windows NT version of the Linux kernel prior to 2.1.63.

Web proxy

Proxy server is a server (a computer system or an application) that acts as an intermediary for request from clients seeking resources from other servers. A client connects to the server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server deleted the request as a way to simplify and control its complexity. An attack occurs on web proxy in different ways: a) Attacker sends requests to web proxy and it attach the proxy to forward the attack request to the victim server. b) The attacker disconnects connection between itself and the proxy server. Three aspects for attackers chose this kind of attacks. It makes possible the attacker to break through the client side governance by connecting different web proxies through HTTP protocols. Detecting this manner of attack in the middle of the web proxies is not a practical approach, apt to lack of synergism contraption between proxy and server, specifically uncontrollable individual proxies This attack may baffle most of the existing discover system designed for the traditional DDoS attacks apt for two reasons: a) the in basis server cannot point blank to observe and recognize the extreme hosts, which are protected by the hierarchical proxy systems. b) The attack traffic is disparate with the habitual client to proxy traffic by every proxy that forwards the traffic.

XSS attack

XSS means Cross-Site Scripting. XSS attacks occurs when an attacker uses a web application to send malignant code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end users browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

XSS attacks occur when: Data enters a Web application through an untrusted source, most frequently a web request. The data is included in dynamic content that is sent to a web user without being validated for malicious content.

Types of XSS attack,

Stored XSS attack: Stored XSS attack is defined as the injected scripts permanently stored on database, visitors log, comment scripts etc. It also referred to as persistent data. Reflected XSS attack: Reflected XSS attack is defined as the injected scripts is reflected off the web server.

III. RELATED WORK

In [1] this paper web proxy based DDoS attack used. Here Hidden Semi-Markov Model (HsMM) parameters used to configure the web access bearing sequence and find which proxy cause attack using temporal and spatial access behavior. On existing system detection of attacks is based only on the proxy server. In such cases, innocent web proxies may blocked. To avoid this problem temporal spatial attack used. This paper proposed a threshold based algorithm called Threshold based attack detection (TBAD) for detecting actual attacking client in HTTP protocol.

In [2] this paper explain how to detect most critical web application security flaws. Web application log files allows a details analysis of a users action. Log files its limits, through. Web server log files contain only a fraction of full HTTP request and response. Knowing these limits the majority of attacks can be recognized and acted upon to prevent further exploitation.

In [3] this paper, we presented detail information of Application Layer Denial of Service Attacks and some of the defense and detection techniques. The major challenge identified in this research is that the application layer Denial of

Service Attacks are harder to get detected. It is because in application layer Denial of Service Attacks the malicious traffic behaves same like that of the legitimate traffic, so it avoids the detection.

In [4] a new server-side defense scheme is proposed to resist the Web proxy-based DDoS attack. Here temporal and spatial locality to extract the proxy-to-server traffic, which is a new problem for the DDoS detection. New scheme was proposed based on TSL. GGHsMM method is use to the improve the detection performance. Main advantages of these system, 1.Detection performance is better than the other methods. 2. it is independent of the traffic intensity and the frequently-varying Web contents. 3. Realize the early detection.

[5] DDoS attack is a very bad threat to the internet. Here detection architecture proposed. in this paper focus on the monitoring web traffic in order to dynamic move in normal traffic, during the flash crowd event signal start App-DDoS attack. The proposed method depend on ICA, PCA HsMM etc. In this paper organized some experiment with different App-DDoS attack modes such as increasing rate attacks, constant rate attack during the flash crowd event. Here duplicate result shows that the system could capture the move of web traffic caused by attacks under the flash crowd event observed the data fitting to the HsMM.

In [6] most of transactions are use on internet. So lots of personal blogs are hack then here provide more security. Using IDS (intrusion detection system) double guard system is used to identify prevent attacks. Using IDS system can provide more security for database server map server using map of demand and query.

In [12] we have presented a survey of the problems of DoS attacks, and the techniques that have been proposed to detect and prevents to these attacks. One important step to contend DoS attacks is to increase the reliability of global network infrastructure.

IV. PROPOSED ALGORITHM

In this paper three algorithm use,
1. Data leakage
2. MD5 Hashing and
3. Static model building.

1. Data leakage algorithm:

Input: Input data D=D1, D2, D3,., Dn saves into the hash table.
Step1: Arrange all input data into matrix format (save into log files.)
Step2: Consider m as a selected data act as a new selected data.
Step3: m position gets changed after allocated time period.
Step4: If Ms data get hacked.
Step5: Data leakage is occurs.
Step6: We have to check the leakage data prevent it.
Step7: Using revert back function we have to get original data.
Step8: When user calls that corrupted file, hash function gives to user a previous data.
Step9: Return true.

2. MD5 Hashing algorithm:

MD5 which stands for Message Digest algorithm 5 is a widely used cryptographic hash function. The idea behind this algorithm is to take up a random data(text binary) as an input and generate a fixed size hash value as the output. The input data can be of any size or length, but the output hash value size is always fixed.
Step1: Start
Step2: For each candidate set element
Step3: For PV(i) CV(i) compare attributes and detect which fields are corrupted
Step4: get who when of corruption event
Step5: prepare a report
Step6: stop.

3. Static model building:

Input: set AQ for database query,
set AR for server query.
Step1: identify the input type of HTTP request whether it is a query or a request
Step2: for each different request do, if r is a request to static file.
Step3: store the input in hash table entry will be

V. SIMULATION RESULTS

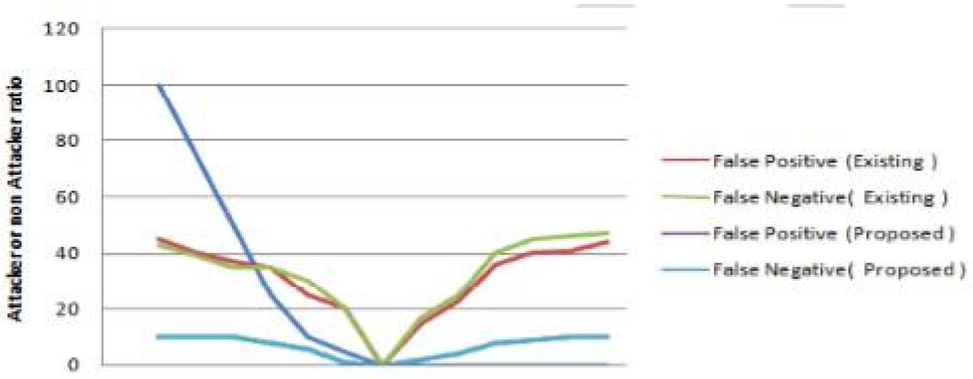

Figure 3: Graphical representation of attacker & Normal client

Figure shows the graphical representation of attacker & Normal client. Both false positive and false negative ratio increases when difference between number of attacking and normal client packets increases. But figure 3 shows that clearly, that it have no effect on current system.

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed study of the http attack on proxy server by using XSS performance. We used here some algorithms and techniques for discovering and protection such as, data leakage, MD5 hashing, static model building etc. This focus on the mapping model for static website using static model building algorithm. It also focus on traffic analysis and behavior analysis.

REFERENCES

1. Dr. K. Kiran Reddy and Dr. P. Bhaskara Reddy, Finding and improvement of user Based HTTP Attacks on Web Proxy by Using SSL performance International Journal of Emerging Trends in Engineering and Development Issue 4, Vol.6 , Oct. - Nov. 2014.
2. Roger Meyer and Carlos Cid, Detecting Attacks on Web Applications from Log Files SANS Institute Reading Room site, 26 January 2008.
3. Shazia Shafi and Sanjay Jamwal, A Review of Application Layer Denial of Service Attacks and Detection Mechanisms, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015, www.ijarcsse.com
4. Yi Xie, S. Tang, Y. Xiang and J. Hu, Resisting Web Proxy-based HTTP Attacks by Temporal and Spatial Locality Behavior, JOURNAL OF L ATEX CLASS FILES, VOL. 6, NO. 1, JANUARY 2007
5. Y. Xie and S. -Z. Yu, Monitoring the Application-Layer DDoS Attacks for Popular Websites,(2009) IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 15-25, Feb. 2009
6. Mr. Chaudhari Hiteshkumar, Prof. Ajay V. Nadargi, DoubleGuard: Detecting Intrusions in Muliti-tier Web Applications, International journal of Advanced Research in Computer and Communication Engg, Vol. 4, Issue 2, February 2015.

7. S. Yu, Hidden Semi-Markov Models, Artificial Intelligence, vol. 174, no. 2, pp. 215-243, 2010.
8. Y. Xie and S. Yu, Measuring the Normality of Web Proxies Behavior Based on Locality Principles, (2008) Network and Parallel vol. 5245, pp. 61-73, 2008.
9. P. Garcia - Teodoro , J. Diaz Verdejo , G. Macia Femandez , and E. Vazquez, Anomaly based Network Intrusion detection: Techniques, Systems and Challenges, computers and security, vol. 28, nos. , pp. 1828, 2009.
10. DoSHTTP, http://www.socketsoft.net/, 2013.
11. Double-guard: detection intrusion in multitier web application Meixing Le, Angelous Starvrou, Member, IEEE, and Brent ByumgHoon Kang, Member, IEEE.
12. Tao Peng, Christopher Leckie, & Kotagiri Ramamohanarao, Survey of network based defense mechanisms countering the DoS and DDoS problems, ACM Comput. Surv. 39,1, Article 3 (April 2007).