SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 155–161

ISSN No: 2454-9614

Low Rate DOS Attack Prevention

S. Kandasamy, N.P. Kaushik*, A. Karthikeyan, S. Aravindh Srira

Department of Computer Science and Engineering,KPR Institute of Engineering and Technology,
Arasur, Coimbatore, Tamil nadu, India.

*Corresponding Author: S.Kandasamy

E-mail: skandu23@gmail.com

Received: 10/11/2015, Revised: 13/12/2015 and Accepted: 03/03/2016

Abstract

"Hacking the Hackers", Nowadays these DoS attacks can be easily detected using many attack detection tools. The Low-rate Denial of service (LRDoS) attacks are a new type of DoS attacks that sends high intensity requests in an ON/OFF pattern to degrade victim's performance and evade the detection designed for traditional DoS attacks. It is more difficult for traditional DoS attack detection method to detect LRDoS attack. The existing system analyzes only the impact of LRDoS attack on a affected system and the existing detection method focus only on TCP related system. A live firewall is managed in the proposed system to monitor all the invoking requests and IP address of the attackers. The Naive-Bayes technique is combined with Priority scheduling concept to produce Classification rules.The proposed system restricts the LRDoS attackers from further accessing the web server. This avoids multiple requests from a same proxy in a particular piece of time and maintains the stability of the web server. Thus the proposed methodology proves as an efficient mechanism to defend the LRDoS attacks on servers.

Keywords: Denial of Service, Attacking systems, Firewall, Packet tracer.

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks can bring down an Internet service, by flooding the high amount of request to the web server. DoS attacks send out high-volume requests to the victim. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. The Quality of Service is the main feature of Internet services, to hack the services of the web server or a website, the attacker uses a Denial of Service (Dos) attack and these Dos attacks nowadays can be easily detected using many attack detection tools. The Low-rate Denial of service (LRDoS) attacks are a new type of Dos attacks that sends high intensity requests in an ON/OFF pattern to degrade victim's performance and evade the detection designed for traditional DoS attacks. LRDoS attacks send out intermittent (instead of continuous) high-volume requests. It forces the victim away from the desired state, thus deteriorating its performance. Moreover, LRDoS attacks can escape the detection designed for flooding-based DoS attacks because of their ON/OFF traffic patterns. It is more difficult for traditional DoS attack detection method to detect LRDoS attack. The request from the LRDoS attacking system and other user request are monitored to understand more about the incoming request. The traffic in the web server is analyzed to maintain the stability state of the website. The data and information which are processed here are used in building a defense mechanism of the web server against the LRDoS attack.

1.1 Objective

The main objective is to prevent the web server from the Low Rate DOS attacks. A live firewall is managed to monitor the incoming request. It filters the Low Rate DOS attack from the user request and restricts the interaction of attackers with the web server.

1.2 Scope

The scope of the project is to analyze and design a system to detect LRDoS attacks on web services running over TCP, UDP and HTTP protocol. It restricts the high privilege instruction from further accessing on the server and maintains the stability of the web server.

2. System Analysis

2.1 Problem Definition

LRDoS attacks send out intermittent high-volume requests to the victim. It forces the victim away from the desired state, thus deteriorating its performance. To prevent the web server from the Low Rate DOS attacks, a live firewall is managed to monitor the invoked request. It filters the Low Rate DOS attack from the user request and restricts the interaction of attackers with the web server.

2.2 Existing System

The existing method analyzes the impact of Low Rate DoS attack on affected system. DoS attack detection tools are unable to detect Low rate DoS attacks. Existing mechanisms require modifications to the infrastructure or protocols which is focus only on TCP related systems.

Disadvantages

- Existing DoS attack detection tools are unable to detect Low rate DoS attacks.
- It only depends on known pattern of attack. It evaluates the impact of Low Rate DoS attack in the web server.

2.3 Proposed System

A live firewall is managed in our proposed system to monitor all requests and IP address of the attackers. Naive-Bayes technique is combined with Priority scheduling concept to produce Classification rules. Router based Firewall use these rules and IP address of the client to filter the LRDoS attack.

Advantages

- Restricting the High privilege instruction from further accessing on the server.

- Avoid multiple requests from a same proxy in a particular piece of time. Maintains the stability of the web server.

2.4 Software Analysis

Microsoft Visual Studio 2012

Introduction to Microsoft Visual Studio2012

Microsoft has a wide variety of products; we designed in ASP.Net and code Written in VB.net for front end designed. And as reports in Crystal Reports is built in Micro Soft Visual Studio 2008. Vb.Net is very flexible and easy to understand any application developer.

2.4.1 About SQL Server 2000

Microsoft SQL Server is a Structured Query Language (SQL) based, client/server relational database. Each of these terms describes a fundamental part of the architecture of SQL Server.

Database

A database is similar to a data file in that it is a storage place for data. Like a data file, a database does not present information directly to a user, the user runs an application that accesses data from the database and presents it to the user in an understandable format. A database typically has two components: the files holding the physical database and the database management system (DBMS) software that applications use to access data. The DBMS is responsible for enforcing the database structure, including: Ensuring that data is stored correctly and that the rules defining data relationships are not violated. Recovering all data to a point of known consistency in case of system failures.

2.4.2 Structured Query Language (SQL)

To work with data in a database, you must use a set of commands and statements (language) defined by the DBMS software. There are several different languages that can be used with relational databases; the most common is SQL. Both the American National Standards Institute (ANSI) and the International Standards Organization (ISO) have defined standards for SQL. Most modern DBMS products support the Entry Level of SQL-92, the latest SQL standard (published in 1992).

2.5 SQL Server Features

2.5.1 Scalability

The same database engine can be used across platforms ranging from laptop computers running Microsoft Windows® 95/98 to large, multiprocessor servers running Microsoft Windows NT®, Enterprise Edition.

2.5.2 Data warehousing

SQL Server includes tools for extracting and analysing summary data for online analytical processing (OLAP). SQL Server also includes tools for visually designing databases and analysing data using English-based questions.

2.6 System integration with other server software

SQL Server integrates with e-mail, the Internet, and Windows.

2.6.1 Databases

A database in Microsoft SQL Server consists of a collection of tables that contain data, and other objects, such as views, indexes, stored procedures, and triggers, defined to support activities performed with the data. The data stored in a database is usually related to a particular subject or process, such as inventory information for a manufacturing warehouse.SQL Server can support many databases, and each database can store either interrelated data or data unrelated to that in the other databases. For example, a server can have one database that stores personnel data and another that stores product-related data. Alternatively, one database can store current customer order data, and another; related database can store historical customer orders that are used for yearly reporting. Before you create a database, it is important to understand the parts of a database and how to design these parts to ensure that the database performs well after it is implemented.

2.7 Overview of the .NET Framework

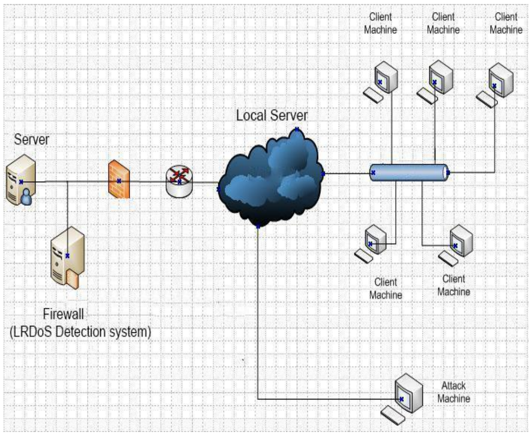
The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet/Intranet. The.NET Framework is designed to fulfill the following objectives: To provide a consistent object-oriented programming environment whether object code is stored and executed locally, executed locally but Internet-distributed, or executed remotely. To provide a code-execution environment that minimizes software deployment and versioning conflicts.

The .NET Framework has two main components:

- **.** NET Framework class library.

3. Overall Architecture Diagram

The overall architecture diagram explains about the proposed system clearly. The user interacts with the web server through the website by providing feedback and also attacker also uses the same website to attack the web server. The firewall which is implemented in between the web server and user will filter the LRDoS attacks from the attacker.



3.1 Algorithm

In the proposed system, the Naive-Bayes algorithm is combined with Priority scheduling concept to filter the LRDoS attack in the Web server. Naive Bayes is a simple technique for constructing classifier models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. It is not a single algorithm for training such classifiers, but a family of algorithms based on a common principle that all naive Bayes classifiers assume that the value of a particular feature is independent of the value of any other feature.

4. Module Description

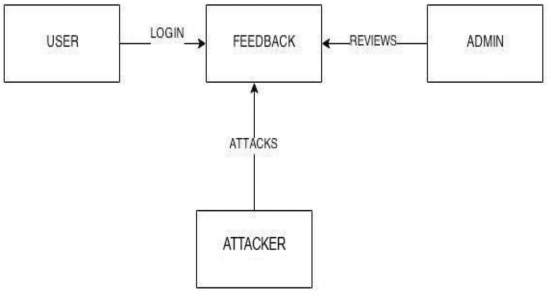
A modular design reduces complexity, facilitates changes (a critical aspect of software maintainability) and results in easier implementation by encouraging parallel development of different part of system. Software with effective modularity is easier to develop because function may be compartmentalized and interfaces are simplified. Software architecture embodies modularity i.e. software is divided into separately named and addressable components called modules that are integrated to satisfy problem requirements.

Modularity is the single attribute of software that allows a program to be intellectually manageable. The five important criteria that enable us to evaluate a design method with respect to its ability to define an effective modular design are: Modular Decomposability, Modular Compensability, Modular Understand ability, Modular Continuity and Modular Protection. The Duos prototype is dealing with the following modules which gives the clear cut description,

- User Registration And Log In
- Online Shopping Website
- LRDoS Attacking System
- Server Control By Admin
- Defending Against Attack Using Firewall
- Request Monitoring System

4.1 Module Explanations

4.1.1 User Registration and Log In



The user needs to register to the website by creating a new account. On registering the username, this module checks the username as it is available in the database or not and provides the proper username. On validating the controls of the user properties, the user credentials are created and the user can able to login into website. Then the modules in the website will be available to the user.

4.1.2 Online Shopping Website

In the website module, there are several panels available to the user through which it can navigate through the different categories such as Home page, Products, Categories(mobile & laptop), and Review. Through the category page, the user will be given various options to select the desired type and can access the details of the product by which they provide proper review to the selected product.

4.1.3 LRDoS Attacking System

In this module, by using the LR-DoS attack tool, we will first connect to the database of the feedback form and acquire the IP address. Then we will input the URL address of the website of the feedback form to input the n number of comments to the feedback database. By providing these false data, the admin and the user will be totally disturbed and various false data may lead to the in quality product and the trust worthiness of the website will be in danger. Thus the user will pose an unworthiness of the website and may degrade the website .By using the LRDoS tool, the website steady state will be disturbed and random feedback will be entered into the module while the feedback will be sent according to the connection type.

4.1.4 Server Control by Admin

In the Admin module, the admin will be able to store the data in the feedback database and maintains the record of the user's feedback. By using the feedback module, the admin shows the feedback of the users by which it matches the best comment for the user's reviews and displays the most relevant comment for the improvements, credits for the user. The admin module provides the necessary conditions for the user feedback by obtaining the name, email, comment. The admin also obtains the IP address of the system by which they acquire the properties of the system

4.1.5 Defending Against LRDoS

A live firewall is managed in this module. It monitors the invoked request and IP address of the user. It restricts the High privilege instruction from further accessing on the server. Avoid multiple feedbacks from a same proxy in a particular piece of time. The admin need to prevent the false data by which the quality of the product as well as the website viewer prediction will be increased as there are more and more trustable feedbacks in the site. Thus we control the feedback by obtaining the each and every system IP address by processing only one comment at a time period of five seconds by using the count and the time of the comment submitted. Thus the admin can able to segregate the true and false data from viewing into the website.

4.1.6 Request Monitoring System

The request from the LRDoS attacking system and other user request are monitored here. This module shows the traffic in the web server. It maintains the stability state of the website.

5. Conclusion

The vulnerability of Internet services to the LRDoS attacks was investigated and the impact of the LRDoS attacks on a web server was also examined. It is proved that the LRDoS attacks can damage the web server and cause loss of time and data. The proposed methodology has proved as an efficient mechanism to defend the LRDoS attacks on web servers by managing a live firewall and mitigating its impacts.

6. Future Enchantment

In future work, the system can be upgraded by enhancing the security provided by the firewalls. Additional security threats can be detected in the further versions. The system can be made compatible with mobile phones and tablets. The project can be upgraded to reduce the time and space complexity by changing the algorithm.

References

[1] A.Sharifi, S. Srikantaiah, A. Mishra, M. Kandemir, and C. Das, "METE: Meeting end-to-end QoS in multicores through system-wide resource management," ACM SIGMETRICS Perform. Eval. Rev., vol. 39, no. 1,p. 13–24, Jun. 2011.

[2] G. Loukas and G. Oke, "Protection against denial of service attacks: A survey," Comput. J., vol. 53, no. 7, pp. 1020–1037, 2010.

[3] G. Loukas and G. Oke, "Protection against denial of service attacks: A survey," Comput. J., vol. 53, no. 7, pp. 1020–1037, 2010.

[4] H. Lim, S. Babu, J. Chase, and S. Parekh "Automated control in cloud computing: Challenges and opportunities," in Proc. 1st Workshop ACDC, Jun. 2009.

[5] W. Chen, Y. Zhang, and Y. Wei, "The feasibility of launching reduction of quality (RoQ) attacks in 802.11 wireless networks," in Proc. 14th IEEE ICPADS, Dec. 2008, pp. 517–524

[6] Y. He, Q. Cao, Y. Han, L. Wu, T. Liu, "Reduction of quality (RoQ) attacks on structured peer-to-peer networks," in Proc. IEEE IPDPS, May 2009, pp. 1–9.

[7] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," IEEE Trans. Inf. Forensics Security, Vol.6, no.2, pp.426-437, Jun.2011.