International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 3, 2022. ISSN: 2348-6600
Reference ID: IJCS-431 PAGE NO: 2878-2880

Mails Management using SMTP Mail Server System

Suryakumar L[#1], Dr. T. Velumani[*2]

[#]*Student, B.Sc Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021*
suryamessi575@gmail.com

[*]*Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021*
velumani.cs@rathinam.in

Abstract - **The project entitled as "Mails Management Using SMTP Mail Server System" has been planned to create in Visual studio.Net as front end and SQL Server as backend. The project aims to develop an Email Server with some salient features such as Access restriction, multi-level user accessing, and email transaction monitoring and additionally identifying the intrusion in the email server. Nowadays, more and more information systems are connected to the Internet and offer Web interfaces to the general public or to a restricted set of users. Such openness makes them likely targets for intruders, and conventional protection techniques have been shown insufficient to prevent all intrusions in such open systems. This paper proposes a generic architecture to implement intrusion-tolerant on email servers. The proposed system having all mail facilities such as send, compose and inbox options. The admin can restrict the right from those features. The admin can monitor all the mailing transactions of every user of the organization. The sender details, receiver details, data, time and date will be stored and can be verified by the administrator. The user will get the intrusion data to their mail. The intrusion data will include the intruder system IP, name and date time along with the tried passwords. This helps to identify the hacker effectively.**

Index Terms – **Access Restriction, E-Mail Server, intruder system IP, Hackers.**

I. INTRODUCTION

Electronic mail is an efficient and increasingly popular communication medium. Like every powerful medium, however, it is prone to misuse. One such case of misuse is the blind posting of unsolicited e-mail messages, also known as spam, to very large numbers of recipients. Spam messages are typically sent using bulk-mailers and address lists harvested from web pages and newsgroup archives.

II. SYSTEM DEVELOPMENT

The problem is thus particularly tricky: on one hand, the development of the Internet allows complex and sophisticated services to be offered, and on the other hand, these services offer to the attacker many new weaknesses and vulnerabilities to exploit. Almost all traditional approaches for building secure systems only focus on preventing attacks to be successful. Such approaches are becoming insufficient when used in the context of open networks like the Internet, which are characterized by frequent appearance of new attacks. Current systems are so complex that it is impossible to identify and correct all their vulnerabilities before they are put in operation. The main aim of the proposed system is the creation of effective Email server for the organization with some additional features. The followings are the features has included in the proposed system.

- Virtual private mail server
- Inbox, outbox, and send items accessibility restrictions.
- Spam detection with customized rules
- Intrusion detection techniques
- Avoids unwanted mails
- Complete process monitoring

This project addresses the issue of anti-spam filtering with the aid of machine learning. this examine supervised learning methods, which learn to identify spam e-mail after receiving training on messages that have been automatically classified as spam or non-spam.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 3, 2022. ISSN: 2348-6600
Reference ID: IJCS-431 PAGE NO: 2878-2880

III. PROPOSED MODULES

Profile Creation:

In this module the profile will be created with the user details like name, address, user id, password and other details. While creating the user profile the admin can specify the access restrictions such as outbox, inbox and send item privileges.

Authentication:

This module is to ensure that the correct user entering and access the resources. The owner can enter and alter the information provided by him. The modules will ask for the password for the authentication.

SQL Query Processing:

The proposed system prevents the complexity against SQL injection attacks. SQL injection is yet another common vulnerability that is the result of lax input validation. The goal of SQL injection is to insert arbitrary data, most often a database query, into a string that's eventually executed by the database. The insidious query may attempt any number of actions, from retrieving alternate data, to modifying or removing information from the database.

Mailing Process:

This module contains the mailing process like composing the new mails and contains the incoming mails and the sent mails process. Spam, folder options will be created in this module.

Spam Detection:

This module helps to identify the spam in the mails. It analyzes the ip address of senders Machine. After analyzing the ip address, messages are sent to the Network Administrator in order to check the activities such as whether it exceeds the user defined rules value. If the resultant activity seems to be abnormal condition, it is then blocked. Otherwise, process continues.

Intrusion Avoidance:

The intrusion is a malicious activities or policy violations. Then there should be an attempt to stop an intrusion attempt. This module is for avoiding intrusion detection by analyzing the rule violation. The person of a company will not be allowed to send any mail to another company without the administrator permission. If the person sends the person mail will be blocked.

Report:

This module contains the report about the activities and the information about the user of the mail server and all other details. The report will be send to the admin. The admin can see the following information.

- User rights
- Send mails and the contents
- Date and time of intrusion
- Blocked accounts etc.,

IV. TESTING METHODS

Unit Testing:

Unit testing focuses verification efforts on the smallest unit of software design, the module. This is also known as "Module Testing" The modules are tested separately this testing is carried out during programming stage itself. In this step each module is found to be working satisfaction as regard to the expected output from the module.

Integration Testing:

Integration testing focuses on the design and construction of the software architecture. Data can be lost across an interface; one module can have adverse effect on another sub functions and show on. Thus, integration testing is a systematic technique for constructing test to uncover errors associated with in the interface. In this project, all the modules are companied and then the entire program is tested as a whole.

Validation Testing:

Validation testing is the requirement established as a part of software requirement analysis is validated against the software that has been constructed. This test provides the final assurance whether the software needs all functional, behavioral and performance requirements. Thus, the proposed system under consideration has been tested by using validation testing and foundto be working satisfactory.

Output Testing:

After performing the validation testing, the next step is the output testing of the proposed system, since no system could be useful if it does not produce required output in the specific format. Tested asking the users about the format required by them, the output is considered into two ways: one is on the screen and the other is printed format.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 3, 2022. ISSN: 2348-6600
Reference ID: IJCS-431 PAGE NO: 2878-2880

The output format on the screen is found to be correct as the format designed according to the user needs, for the hard copy also, the output comes as specified by the user. Hence output testing does not resultin correction in the system.

User Acceptance Testing

User acceptance testing of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keep in touch with the prospective system user at time of developing and making changes wherever required.

System Implementation

In this project, propose virtualizing Harvard architecture on top of the existing memory architecture of modern computers, including those without non-executable memory page support, so as to prevent the injection of malicious code entirely. Harvard architecture is simply one wherein code and data are stored separately. Data cannot be loaded as code and vice-versa. In essence, we create an environment where in any code injected by an attacker into a process' address space cannot even be addressed by the processor for execution.

In this way, we are attacking the code injection problem at its root by regarding the injected malicious code as data and making it unaddressable to the processor during an instruction fetch. Split memory architecture produces an address space where data cannot be fetched by the processor for execution. For an attacker attempting a code injection, this will prevent him from fetching and executing any injectedcode.

V. CONCLUSION

It is concluded that the application works well and satisfy the needs. The application is tested very well and errors are properly debugged. Finally, our proposed system having all mail facilities such as send, compose and inbox options. The admin can restrict the right from those features. The admin can monitor all the mailing transactions of every user of the organization. The sender details, receiver details, data, time and date will be stored and can be verified by the administrator. The user will get the intrusion data to their mail. The intrusion data will include the intruder system IP, name and date time along with the tried passwords. This helps to identify the hacker effectively.

REFERENCES

[1] OpenStack Installation Guide for Ubuntu 14.04. (n.d.). Retrieved November 20, 2016, from http://www.docs.openstack .org/juno/install-guide/install/apt/content/

[2] Adam. (2013, September 8). Creating a Mail Server on Ubuntu. Retrieved from http://www.pixelinx.com/

[3] Email Sending Limit and Send Rate – Gmail, Hotmail, Yahoo! Mail, AOL. (n.d.). Retrieved November 20, 2016, from http:// www.yetesoft.com/free-email-marketing-resources/email- sending-limit/

[4] Operator Training Guide. (n.d.). Retrieved November 20, 2016, from http://docs.openstack.org/ icehouse/training-guides/con tent/bk_operator-training-guide.html

[5] I. Forster, J. Larshon, M. Masrich, A. Snoerean, S. M. Savage, and K. Levchenkro. Security by many other names: On the effectiveness of the provider based email security. In 22nd ACM Conference on the Computer and Communications Security, Oct. 2015.

[6] Klenshin, (2001) 'Simple Mail Transfer Protocol on Internet' IETF RFC 2821.