Full-Automated Spam Mail Removing Linux-Based Email Server System

WKA Thamel[#1]

[#1]*Department of Computing and Information Systems, Faculty of Applied Sciences,*
Sabaragamuwa University of Sri Lanka, Belihul Oya.

[#1]*<thamel.syinfo@gmail.com>*

Abstract — Spam mail generating and spreading is happening on email servers. There is no fully automated mechanism to remove the generated spam mails and normalize the email queues without the interaction of humans. Then System Administrator has to reset the password of the infected mail address. On this research, our objectives are to remove the generated spam mails from mail queue, reset the password if infected mail address fully automated and notify to the System Administrator via a simple notification email. Here we are using the mail removing mechanism according to the threshold value and reset the login credentials according to the username of the email address.

Once the threshold value was exceeded the on of email address, the system will remove the generated spam emails and normalize the email queue. Then the system will generate the random password for that compromised email address using the first three letters of the email id, first three letters of the domain name and the date that mail id was compromised. Then send the new login credentials to the System Administrator via simple notification email. [We can adjust the threshold value according to the email id list.] From this research we were able to reduce the spam mail spreading to the other servers. Also, we have implemented this mechanism for the corporate level email servers and got successful results. And it was helpful to keep the good reputation of the email server IP address and avoid the domain name blacklisting on RBLs.

.

Keywords— Spam, Automated, Threshold, Credential, RBL

I. INTRODUCTION

Software industry is much younger and knowledge intensive industry which mostly depends on the knowledge resource. Most of the software companies are profit-oriented organizations. Even, these companies are still under development, they have a great aspiration to grow and achieve sustainability in market. Generally, these companies are project-based companies and therefore, ultimate success of the business depends on the success of projects they undertake, and the success of these projects could be achieved only through satisfying the customers by completing these projects successfully within the budgeted time and cost. Therefore, these companies consider successful project completion and customer satisfaction as their short-term goals. By means of customer satisfaction, they achieve the sustainability in the market which is considered to be the long-term goal of a software company. (Xianghan Zhengab, Zhipeng Zengab, Zheyi Chenc, Yuanlong Yuab, Chunming Rongd, 2015)

Emails allows you to, at no cost, send a letter of unlimited length to one person or many people at once. It arrives almost instantly, and they can reply straight away. Setting up your own email account will allow you to communicate with people you know in ways you never thought possible. While you will have heard of email, you may not know exactly how it works, what you need to get set up, or how to use it. You won’t have an existing email account, either. Spam is increasingly sent from computers infected by computer viruses.

Virus-makers and spammers are combining their efforts to compromise innocent computer users’ systems and converting them into spam-sending “drones” or “zombies”. These malicious programs spread rapidly and generate massive amounts of spam pretending to be sent from legitimate addresses. It’s important for all computer owners to install and maintain anti-virus software to avoid having their computer infected and possibly become a source of spam without their knowing. Effects of spam. Aside from the amount of junk arriving in the Inboxes of millions of innocent email users every day, spam can have a more indirect and serious effect on email services and their users.

Spammers harvest recipient addresses from publicly accessible sources, use programs to collect addresses on the web, and simply use dictionaries to make automated guesses at common usernames at a given domain. Spamming is politically debated in several countries and has been legislated some places with varying results.

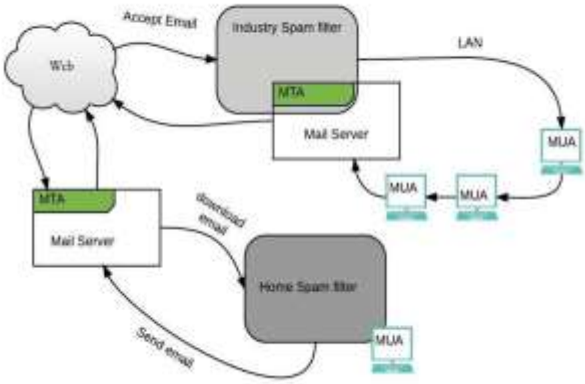
The primary objective of this study is to provide a more complete and a comprehensive description of the knowledge sharing behaviour and the obstacles against knowledge sharing practices in Sri Lankan software industries engaged in software development by following a survey based empirical research method. In order to achieve this goal following research questions (RQs) are proposed.

RQ1. What is the currently using mechanism for Avoid IP blacklisting, Domain blacklisting of Linux Based email server systems?

RQ2. What are the barrier factors which affect Spam mail removing from Linux based email server systems?

RQ3. What is the effect from each barrier factor towards Spam mail removing from Linux based email server systems?

RQ4. What are the solutions and improvements to be implemented on Linux based email server systems, in order to remove the effect from each barrier factor towards Linux based email server systems?



This research presents a literature study that integrates studies of current status of Spam mail generating of Linux based email server systems and how to fully automate remove the generated spam mails from Linux based email server systems. (Hanif Bhuiyan, n.d.)

II. LITERATURE REVIEW

A spam firewall is a single box computing appliance that is set up in front of the email server. This appliance receives all the incoming email for the organization and processes it such that only the good email is passed on to the email server. A spam firewall is normally built on a hardened operating system based on Linux or BSD. However, some vendors do make solutions based on other operating systems. The appliance format and the hardened operating system make the spam firewall less susceptible to hackers and other threats. A proper spam firewall protects the email server from all forms of attack in addition to filtering spam. At the most basic level, a spam firewall blocks unwanted email from entering the network and reaching the email server. This is accomplished using a multi-layered filtering solution. Some spam firewalls use only a single technology for eliminating spam. However, this is not preferred since spammers find it easier to work around a single technology. In most cases spam firewalls are designed to block inbound spam. Then spam Firewall IP (Internet Protocol) will blacklisted on bad reputation of mail server. Spam firewalls do not act as corporate stronghold to the network. (S. Dhanaraj ; V. Karthikeyani, 2013)

Itself and should not take the place of a standard Internet firewall. An Internet firewall is set up to limit access to the network via the many protocols that can be used to attack an organization. A spam firewall only defends against attacks on SMTP (Simple Mail Transfer Protocol) port 25. Furthermore, a spam firewall is not an SMTP relay. It is designed only to protect the email server. If it has multiple functions, such as operating as an outbound relay, it may compromise the security it provides to the email server. For example, traditional firewalls very rarely function as routers; to do so would compromise their ability to act as a firewall. (Yehonatan Cohen Daniel Gordon Danny Hendler, 2018)

A spam firewall is typically housed within the DMZ, between the Internet router and the corporate email server. There are several different ways in which a spam firewall can be installed and deployed depending on the needs of the organization. Standard deployment involves simply connecting the spam firewall to the corporate network by assigning it a new IP address. Once the IP is configured the corporate MX records are adjusted to point to the new IP of the spam firewall. The Spam Firewall comes pre-configured and begins operating with no additional adjustments. The web interface can be used to further tune or enable additional features.

Symantec Email Security, SpamFighter, SpamAssassin, PureMessage, GFI MailEssentials, Check Point Email Security, SonicWALL Email Security, Cyberoam Email Security, Luxsci, Vipre Email Security, CYREN Email Security, SecurityGateway, Mailwasher Pro, Exclaimer Anti-Spam, SpamExperts and all other "Spam Firewalls" are detecting spam mails. All above spam firewall subscriptions are highly cost [Non-Open Source]

III. TECHNOLOGY

Moreover, this study focuses on the concept, 'Theory of Planned Behaviour' (TPB); an extended concept of predicting behaviour in any social situation; and applies this theory as the basement of this research work. It is expected that the findings derived through this study will provide useful information for both academics and practitioners to better understand knowledge sharing behaviour in software companies in the context of Sri Lanka. The contribution of this empirical study consists of baseline data and recommendations that could be a source of general guidance for academic researchers in stimulating future research in the subject of knowledge sharing.

Taking previous researches and mechanism regarding spam mail receiving and how to block the spam mails from spam filter gateways or inbuilt mail scanners. Still there are no mechanism for prevent from the spam mail generating. Also, there are no mechanism for remove the generated spam mails from server and normalize the mail queues.

1. Commercial spam mail filtering gateways.

Basically, spam filter gateways implement for the filter the incoming mails and deliver the legitimate mail to the email server. Nowadays Spam filter gateway providers provide their solution for clean the outbound mails, from that way they are trying for reduce the spam mails delivering tot the outside domains. It will be helpful to the keep good reputation for their domain and IP address blocks too. Also, these devices are another hardware devices or cloud-based solutions. [Barracuda spam filter gateways (Hardware and Cloud based), Forti-Mail spam filter gateways (Hardware and Cloud based)] (Emeka W. Dumbili, 2015)

2. Open Source spam mail filtering mechanisms.

Basically, MailScanner solution using for install on opensource email servers. Then system engineers are customizing the spam mail filtering rules. From this mechanism we can reduce the receiving spam mails. Also, this solution not similar to this research. (Hamoon Takhmiri Ali Haroonabadi, 2016)

IV. DISCUSSION

According to the results of the above-mentioned automated system, it's not suitable for the bulk mail server systems, because bulk mail senders are sending more than thousands of mails to the thousands of recipients at once. When bulk mail email server was compromised, we cannot troubleshoot that issue without login to the email server system. Best spam mail generating avoid mechanism is implement the complex password with more than 20 characters. Also, bulk email server system's mail queue is always high mail queue and it always exceeding the threshold value. If we implement the bulk email server system with above mechanism, bulk mail senders cannot send their mails to the recipients and all mails will remove from the email queue.

Also, we have to restrict the maximum recipients per email, because sometimes local staff mails are sending with more than hundred recipients, if they send mails with above mentioned conditions staff mails will identify as the spam mails. To avoid this issue, we can exempt the local domain names from the automated system. That means local mail senders can send unlimited emails at once with unlimited recipients.

Using this fully automated anti-spam mail generating server we cannot block, delete or reject the inbound spam mails, spoofing mails and virus mails. Because this server system is not working as a spam filter or advance threat protection [ATP] or RBL referring MailScanner. Also, this server system is not referring the clam AV or spam assassin rules for detect the generated spam mails. This server system is referring local reputations only and server system working for control the bad reputations of the email server system.

If, Zimbra email servers have recommended specification [if server was implemented on VMware environment recommended vCPU count was 4 and Memory was 8 GiB, if server was implemented on Hardware environment recommended processor was intel Xeon and memory was 8 GiB] this automated system is running without the resources utilization, when the spam mails were generated resource utilization was not increased.

If too much mails were delivered to the global mail server from unique mail id, real time blacklisting [RBL] monitor these mails and identify it as a spam mails are generating from that server IP address and block it. Basically "Barracuda RBL, Zen RBL, CBL, SpamHouse, Trent Micro and etc." are do the real time black listing. From this research we can avoid this, because server able to remove the generated spam mails, before the delivering.

If too much mails were delivered to the global mail server from unique mail id, real time blacklisting [RBL] monitor these mails and identify it as a spam mails are generating from that domain and block it. Basically "Barracuda RBL, Zen RBL, CBL, SpamHouse, Trent Micro and etc." are do the real time black listing. From this research we can avoid this, because server able to remove the generated spam mails, before the delivering.

When the server IP was black listed on RBL's sometimes system admins must pay for remove the IP from RBLs. As a solution Internet service provider [ISP] are add a "Source NAT" for that infected server IP. Once that server identified as a spam generating source, NAT IP will be blacklisted again. ISP can add another NAT as an alternative solution. If that IP was blacklisted again, RBL's will blacklist the whole IP block. [any subnet, /24, /29 or any other subnet].

From that automated anti-spam removing method, system admin doesn't need to find the infected mail id, delete the generated spam mails from server, reset the password of infected mail id, restart the SASL Authentication services. All thing will be happening fully automatically.

From that automated anti-spam removing method, it deletes the generated spam mails and normalize the mail queue into the recommended value. Doesn't need to throttle the mail queues.

If mail server delivering too much mails to the global servers, it will be identified as a bad reputation. From this method mails are delivering to global mail servers with a control. (News, 2007)

ACKNOWLEDGEMENT

I am highly indebted to many individuals for their guidance and constant supervision they provided during the course of this research work.

First of all, I would like to express my deepest gratitude towards my supervisor Mr. R.L. Dangalla, Lecture in Department of Computing and Information Systems, Faculty of Applied Sciences in Sabaragamuwa University of Sri Lanka, for his assistance, encouragement, guidance, and continuous concern over each step during this research period for making this a success.

Also, I would like to give my gratitude and thanks to the staff members of Department of Computing and Information Systems for their valuable help and kind guidance.

And I am immensely grateful to the selected companies who provided their spam mail related issues to me and others who assist me on the pilot test and provided their comments for making it a more reliable and accurate one.

Finally, I give my sincere gratitude to my parents and colleagues who provide me the moral and emotional support in my life and for their kind co-operation and encouragement which help me in succeed of any life event.

CONCLUSION

This study mainly focuses on avoid the spam mail generating and spreading the spam mails to the outside domains. From this fully automated anti-spam mail generating we can reduce the ip address blacklisting and domain name blacklisting in RBLs. Also, from this mechanism we cannot stop the ip address blacklisting and domain name blacklisting. Because, this system allows the legitimate mails to the outside and it's not filtering the mails from the actual body content of the email. If an organization send their mails similar to the advertisements, these mails will identify as the marketing mails and RBLs will put the server IPs and domains to their lists.

RFERENCES

Emeka W. Dumbili, 2015. How can one avoid emails from predatory journals/publishers that solicit for articles?

Hamoon Takhmiri Ali Haroonabadi, 2016. Identifying valid email spam emails using decision tree. Int. J. Comput. Appl. Technol. Res. 5, 61–65.

Hanif Bhuiyan, n.d. A standard process of Email spam filtering system.

Manajit Chakrabortya, Sukomal Pala, Rahul Pramanikb, C.Ravindranath Chowdary, 2016. Recent developments in social spam detection and combating techniques: A survey. Inf. Process. Manag. Volume 52, 1053–1073.

News, 2007. Spam formats shift again. 349 Volume 2007, 2.

Research Focus, 2008. Research Focus: The fuelling of spam through email placement. Comput. Fraud Secur. 2008, 4.

S. Dhanaraj ; V. Karthikeyani, 2013. A study on e-mail image spam filtering techniques. IEEE - 2013 Int. Conf. Pattern Recognit. Inform. Mob. Eng.

Xianghan Zhengab, Zhipeng Zengab, Zheyi Chenc, Yuanlong Yuab, Chunming Rongd, 2015. Detecting spammers on social networks. https://doi.org/10.1016/j.neucom.2015.02.047 Volume 159, 27–34.

Yehonatan Cohen Daniel Gordon Danny Hendler, 2018. Early detection of spamming accounts in large-Scale service provider networks. Knowl.-Based Syst. 142, 241–255.