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

WKA Thamel

Department of Computing and Information Systems, Faculty of Applied Sciences, Sabaragamuwa University of Sri Lanka, BelihulOya
*thamel.syinfo@gmail.com

The generating and spread of spam mail happens on email servers. There is no fully automated mechanism to remove the generated spam mails and normalize email queues without the interaction of humans. Then System Administrator has to reset the password of the infected mail address. The objectives of this study are to remove the generated spam mails from mail queue, reset the password fully automated if mail address is infected and notify System Administrator via a simple notification email. The mail removing mechanism is used according to the threshold value and reset of login credentials are according to the username of the email address. Once the threshold value exceeds the email address, the system will remove the generated spam emails and normalize the email queue. Then the system will generate a 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, the new login credentials will be sent to System Administrator via a simple notification email. [threshold value can be adjusted according to the email id list.] This study was able to reduce spam mail spread to the other servers. Also, the study has implemented the mechanism for corporate level email servers and received successful results. 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