Security Tools Lab 2

Project 4 – Email Spam Filtering Techniques (46 pts)

This project can be done by a single student.

A phishing email is an unsolicited email that attempts to remain undetected by exploiting human unawareness in order to steal sensitive information about a user. To prevent phishing emails from reaching the end users' inbox, spam filters are used as protection. These filters include features such as scanning and analysis of emails content, authentication of senders, policy validation and statistical analysis. While content is a very important part of phishing emails detection, other aspects must be considered in order to filter phishing emails more efficiently. We have seen SMTP security extensions like SPF, DKIM and DMARC emerging in the early years of the 21st century to counter email spoofing.

In this project, you will assess how emails are classified as spam and determine which phishing emails characteristics are examined by spam filters. Due to the difficulties of experimenting with proprietary solutions, we will limit ourselves to experimenting with two largely used open-source spam filters, namely Apache SpamAssassin and Rspamd. You can use default configuration, default rules, and no extra plugins. Your study is not focusing on the content of email bodies but rather on email headers triggering of rules. You can experiment with Jose's phishing email dataset (https://monkey.org/~jose/phishing/) or you can use your own dataset. Compare the performance of the two software as well as the triggered rules and their scoring systems.

After identifying which spam filter rules, other than those that are content-specific, are triggered by the email, you will then research how to lower the score given to the email by the two spam filters, to avoid detection and classification as spam. Finally, after determining and implementing a solution to bypass the spam filters' protections, you will test your solution with a subset of emails against the spam filters of the known email service providers such as Office365, Gmail and/or your own organisation's solution. Evaluate and discuss your results.

- Implementation – 16
- Complexity of Work – 10
- Effectiveness of Solution - 10
- Report - 10