Phishing Detection Using Email Parsing and Machine Learning

1. Introduction

Phishing attacks are a prevalent and dangerous threat in cybersecurity, where attackers deceive individuals into revealing sensitive information through fraudulent communications. This project aims to build a phishing detection system that utilizes email parsing, URL extraction, and machine learning techniques to identify and classify phishing attempts.

2. Project Objectives

- Email Parsing : Extract and process email content to analyze its structure and content.

- URL Extraction : Identify and extract URLs from email content for further analysis.

- Phishing Detection : Implement a basic detection mechanism to classify emails as phishing or legitimate.

- Machine Learning Integration : Enhance the detection system by incorporating machine learning for improved accuracy.

3. Methodology

3.1 Email Parsing

Objective : Extract content from emails to prepare for phishing detection.

Approach :

1. Connect to the Email Server : Use IMAP to connect to the email server and access the inbox.

2. Fetch Emails : Retrieve email messages from the inbox.

3. Parse Email Content : Extract the subject and body from each email, handling both plain text and multipart messages.

3.2 URL Extraction

Objective : Identify URLs within email content to detect potential phishing links.

Approach :

1. Extract URLs : Use regular expressions to identify and extract URLs from the email body.

2. Validate URLs : Optionally, validate URLs to check for known phishing domains or suspicious patterns.

3.3 Basic Phishing Detection

Objective : Implement a basic mechanism to identify phishing attempts based on email content.

Approach :

1. Keyword Matching : Use keyword matching to identify common phishing indicators in the email subject and body.

2. Classify Emails : Mark emails as phishing if they contain suspicious keywords or patterns.

3.4 Machine Learning Integration

Objective : Improve phishing detection accuracy by applying machine learning techniques.

Approach :

1. Data Preparation : Collect and preprocess email data, including text cleaning and feature extraction.

2. Feature Extraction : Convert email text into numerical features using techniques like TF-IDF.

3. Model Training : Train a machine learning model (e.g., logistic regression) on labeled email data to classify emails as phishing or legitimate.

4. Model Evaluation : Assess the performance of the model using metrics like accuracy, precision, recall, and F1-score.

4. Results

1. Email Parsing :
   - Successfully extracted email subjects and bodies.
   - Managed both plain text and multipart emails.

2. URL Extraction :
   - Identified and extracted URLs from email content.
   - Validated URLs to detect potentially harmful links.

3. Basic Phishing Detection :
   - Implemented keyword matching to detect common phishing indicators.
   - Successfully classified emails based on predefined keywords.

4. Machine Learning Integration :
   - Preprocessed email data and extracted features.
   - Trained a logistic regression model with email data.
   - Evaluated model performance and achieved satisfactory results.

5. Conclusion

The phishing detection system successfully integrates email parsing, URL extraction, and machine learning to identify phishing attempts. The system can be further enhanced by incorporating more advanced machine learning algorithms, real-time email processing, and additional phishing detection features.

Future work includes:

- Enhancing the phishing detection model with more sophisticated techniques.
- Implementing real-time email parsing and phishing detection.
- Exploring cloud-based deployment options for scalability.