Phishing Attack Simulation and Detection using Python

Project Details

Name: Periyasamy S
College: Sasurie College of Engineering
Department: B.E Computer Science and Engineering (Cybersecurity)

Abstract

Phishing attacks are one of the most common cyber threats used to steal sensitive information such as usernames, passwords, and banking details. This project focuses on simulating phishing attacks and detecting them using basic Python logic. The system analyzes email content and identifies suspicious keywords and patterns to classify emails as phishing or legitimate.

---

1. Introduction

With the rapid growth of internet usage, cyber crimes have increased significantly. Phishing is a type of social engineering attack where attackers trick users into revealing confidential information. This project helps in understanding how phishing attacks work and how they can be detected using simple programming techniques.

---

2. Objective

To understand phishing attack techniques

To simulate phishing emails for educational purposes

To detect phishing emails using Python

To create cybersecurity awareness

---

3. Tools and Technologies Used

Python Programming Language

Visual Studio Code / Any Python IDE

Sample Email Data

GitHub

---

4. Methodology

1. Collect sample phishing and legitimate email contents

2. Convert email text into lowercase for uniform analysis

3. Define a list of commonly used phishing keywords

4. Check email content for suspicious keywords

5. Classify the email as Phishing or Legitimate

---

5. Implementation

The phishing detection logic is implemented using Python. The program scans email content and checks for commonly used phishing keywords such as "urgent", "verify", and "password". If any keyword is detected, the email is marked as phishing.

---

6. Sample Code Logic

The sample code works by analyzing the content of an email and searching for commonly used phishing keywords. First, the email text is converted into lowercase to ensure accurate comparison. A predefined list of phishing-related keywords is created. The program checks whether any of these keywords are present in the email content. If a match is found, the email is classified as a phishing email; otherwise, it is considered legitimate.

Sample Python Code

List of common phishing keywords

```
phishing_keywords = [
"urgent",
"verify",
"account",
"password",
"click here",
"login",
"bank"
]

def detectphishing(emailtext):
emailtext = emailtext.lower()
for keyword in phishing_keywords:
if keyword in email_text:
return "Phishing Email Detected"
return "Legitimate Email"

sample_email = "Your account is blocked. Please click here to verify immediately."
print(detectphishing(sampleemail))
```

---

6. Results

The system successfully detects phishing emails based on predefined rules. Sample outputs show clear identification of phishing attempts, helping users understand common phishing patterns.

---

7. Applications

Cybersecurity awareness training

Educational demonstrations

Basic email filtering systems

Beginner-level cybersecurity projects

---

8. Conclusion

This project demonstrates that phishing attacks can be detected using simple Python logic. Although the system uses basic rule-based detection, it provides a strong foundation for understanding cybersecurity concepts. The project can be enhanced further using machine learning techniques.

---

9. Future Enhancements

Implement machine learning for better accuracy

Analyze URLs and email headers

Create a web-based interface using Flask

---

10. References

https://owasp.org

https://www.kaspersky.com

https://www.geeksforgeeks.org