SMART INDIA HACKATHON 2022

Basic Details of the Team and Problem Statement

Ministry/Organization Name/Student Innovation:

Ministry of External Affairs (MEA)

PS Code: **LC1076**

Problem Statement Title: **Email Spoofing Detection**

Team Name: **KuroBulls**

Team Leader Name: **Vani Seth**

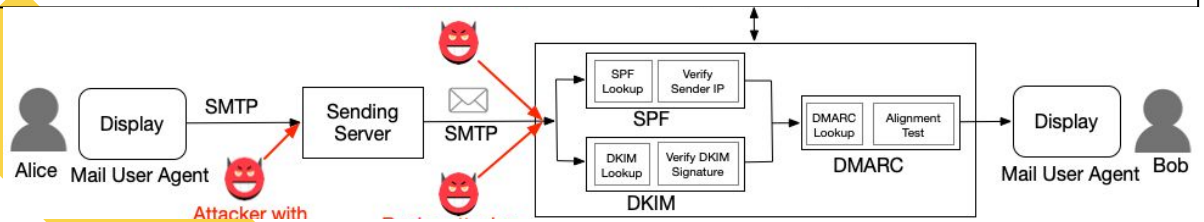
Institute Code: **U-0275**

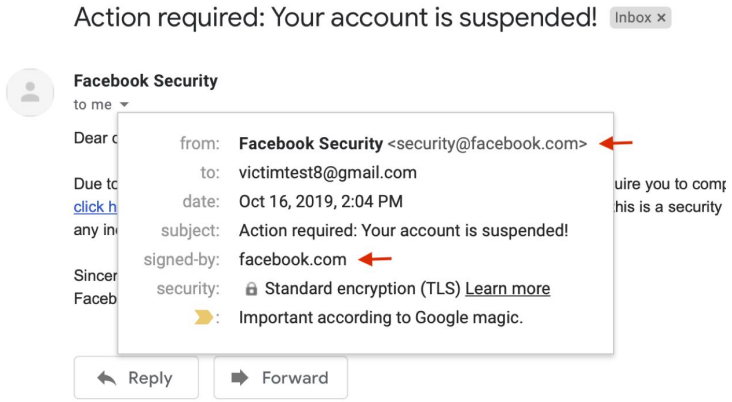
Institute Name: **Jaypee University of Engineering and Technology, Guna**

Theme Name: **Blockchain and Cybersecurity**

Idea/Approach Details

- Our project aims to resolve the problem of email spoofing at the server itself.
- Our approach includes adding a module to existing servers to check whether the received email is spoofed or not by using various custom features used for determining whether the received email is suspicious or not. After cross checking it with IP tracing and various parameters the server will either discard or allow the mail to proceed. The email will arrive on server and will be filtered out if it is spoofed.
- We aim to build our project further by adding various other parameters and establishing a database where the logs of emails will be stored.
- These logs will help big organizations like Google, Yahoo etc. to check how many spoofed emails are sent by using their domain names. It will help to trace out the which are responsible for sending the spoofed emails.





Describe your Technology stack here:

- Python
- SET (Social Engineering Toolkit)
- Hmail Server
- Thunderbird
- NLP
- WhoIs API
- Kaggle
- Postmark's DMARC REST API

Idea/Approach Details

- Our approach includes two ways of verifying whether the email is spoofed or not.
- Primary approach includes retrieving IP addresses and checking whether it comes from a trusted domain or not.
- Additionally, what makes our approach stand out is using flagging parameters which will filter out spoofed emails based on various hybrid features at the server only. (Mentioned beside)
- Based on conclusions from the result of the flagging parameters the server will filter out the spoofed email.
- We are also using the SPF (Sender Policy Framework), DKIM(Domain Key Identified Mail) and DMARC(Domain-based Message Authentication, Reporting and Conformance) protocols to identify the spoofed emails.

Some Features Used:

- Blacklist words in title, such as bank, pay, account, password.
- inconsistency between replier's address and the sender's address.
- Inconsistency between sender domain and Message-Id domain.
- Checking if the email is in the HTML format.
- The number of "%" character in URL.
- Inconsistency between where the URL actually leads to and the text the link appeared.
- The psychological features in email.

  etc.

Team Member Details

Team Leader Name: Vani Seth

Branch (Btech/Mtech/PhD etc): Btech | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): II

Team Member 1 Name: Tanish Khandelwal

Branch (Btech/Mtech/PhD etc): Btech | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): II

Team Member 2 Name: Vaibhav Singh Rajpoot

Branch (Btech/Mtech/PhD etc): Btech | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): II

Team Member 3 Name: Utkarsh Mathur

Branch (Btech/Mtech/PhD etc): Btech | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): II

Team Member 4 Name: Sonali Rajput

Branch (Btech/Mtech/PhD etc): Btech | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): II

Team Member 5 Name: Satyam Kumar

Branch (Btech/Mtech/PhD etc): Btech | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV):II