Tutorial No. 2

Title: Compile reporton Phihsing attacks

Roll No.: 16010423076 **Experiments No.:2**

Aim : Compile a comprehensive report on Phihsing attacks

Theory:

Phishing is a type of online scam where attackers try to steal sensitive information like passwords, credit card numbers, or personal details. They often trick people into clicking on fake emails, websites, or links that look real. These scams can happen through email, social media, or even text messages. The goal of phishing is to get people to share private information without realizing they are being tricked.

Concept of Phishing

Phishing relies on psychological manipulation, often exploiting trust or fear. Attackers design scams to mimic legitimate communications, making victims more likely to respond. For instance, they may impersonate a trusted institution like a bank or government agency. By crafting messages with urgency—such as warnings about account suspension—attackers push victims to act without thinking critically. Understanding this concept helps us recognize the deceptive strategies used in phishing.

Types of Phishing Attacks

There are different types of phishing attacks. One of the most common is **email phishing**, where attackers send fake emails pretending to be someone trusted like a bank or a company. Another type is **spear phishing**, which targets specific people or organizations. **Vishing** is a phone-based phishing attack, while **smishing** involves text messages. **Clone phishing** occurs when attackers duplicate a legitimate message and alter the content to include malicious links or attachments. Additionally, **whaling** targets high-profile individuals like CEOs or government officials. Each of these methods uses tricks to make the attack look real, making it harder to spot.

How Phishing Attacks Work

Phishing attacks usually work by sending fake messages that appear to be from a trusted source. The attacker might ask the victim to click on a link or download an attachment. These links often lead to fake websites that look like real ones. Once the victim enters their information, the attacker steals it. The trick is to make everything seem authentic, so the victim doesn’t realize they are being scammed.

How to Create Phishing Pages

Creating phishing pages involves replicating legitimate websites to deceive users into providing sensitive information. Attackers use tools to clone webpages, copying design elements, logos, and forms. These fake pages are then hosted on malicious servers, often

using URLs similar to the original sites to avoid suspicion. While learning about these techniques is critical for cybersecurity research and education, such knowledge must be applied ethically and solely for defensive purposes.

Phishing Databases

Phishing databases play a crucial role in identifying and combating phishing attacks. These databases collect and maintain records of known phishing websites, email templates, and attack patterns. Security tools and web browsers use these databases to block malicious websites and warn users. For example, services like PhishTank allow users to report and verify suspected phishing URLs, contributing to a global effort to reduce phishing threats.

Consequences of Falling for Phishing

Falling for phishing can have serious consequences. If someone shares sensitive information like passwords or bank details, attackers can steal money, access personal accounts, or commit identity theft. This can lead to financial loss and a lot of stress. In some cases, falling for phishing can also harm the victim's reputation, especially if the attacker uses their information for fraud.

Phishing Prevention and Detection

To avoid falling for phishing attacks, it's important to be careful when receiving emails or messages from unknown sources. Always check if the website looks real before entering any information. Look for signs like strange URLs or spelling mistakes. Installing security software and using strong, unique passwords for every account can also help protect against phishing. It's important to stay aware of new scams and learn how to recognize them.

Advanced Trends in Phishing Attacks

Phishing is evolving with advancements in technology. Attackers now use **artificial intelligence (AI)** to generate convincing emails and mimic human-like interactions. Deepfake technology allows attackers to create fake voice or video messages, making scams more believable. **Phishing-as-a-Service (PhaaS)** platforms are emerging, enabling attackers with limited skills to purchase pre-made phishing kits. Additionally, sophisticated techniques like multi-channel phishing—combining email, SMS, and phone calls—are making attacks harder to detect.

Case Studies of Notable Phishing Attacks

One famous phishing attack was the 2016 phishing scam that targeted employees of the Democratic National Committee (DNC) in the U.S. Attackers used a fake Google login page to steal login details. This attack led to the hacking of emails that were later leaked. Another example is the 2017 phishing attack on Target customers, where scammers stole credit card information from millions of people by sending fake emails. These cases show how dangerous and widespread phishing can be.

Emerging Trends in Phishing

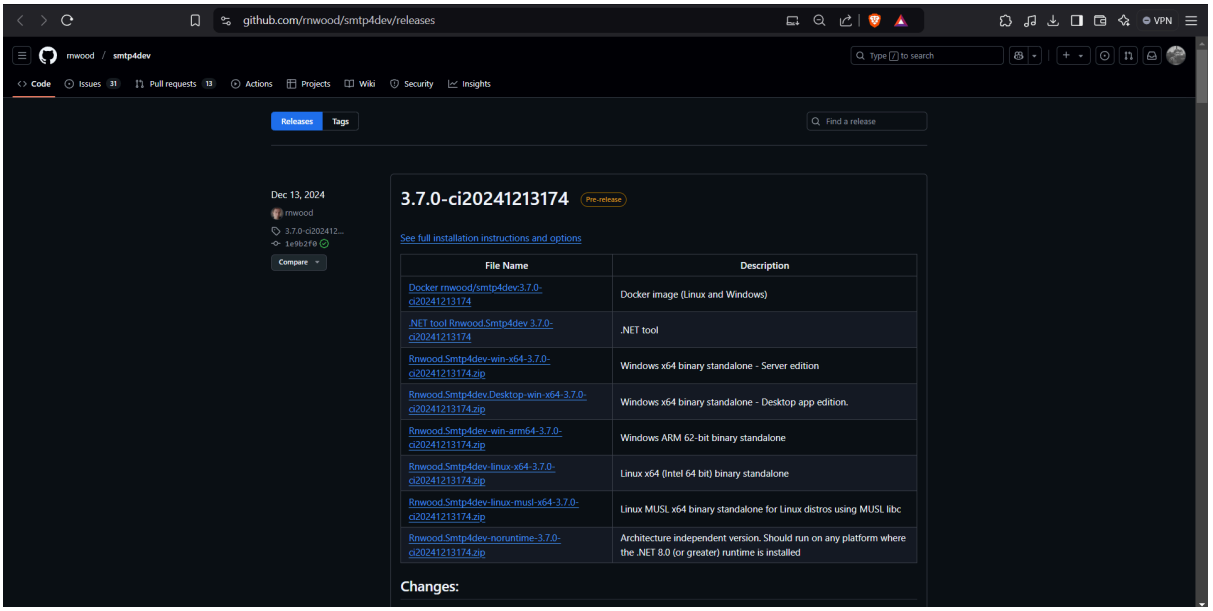
Phishing attacks are constantly evolving. One new trend is **"whaling,"** which targets high-profile individuals like CEOs or government officials. Attackers also use more sophisticated techniques like deepfake technology to make voice or video calls seem real. Another emerging trend is the use of artificial intelligence to create fake messages or websites that are harder to detect. As technology improves, phishing attacks are becoming more convincing and harder to spot.

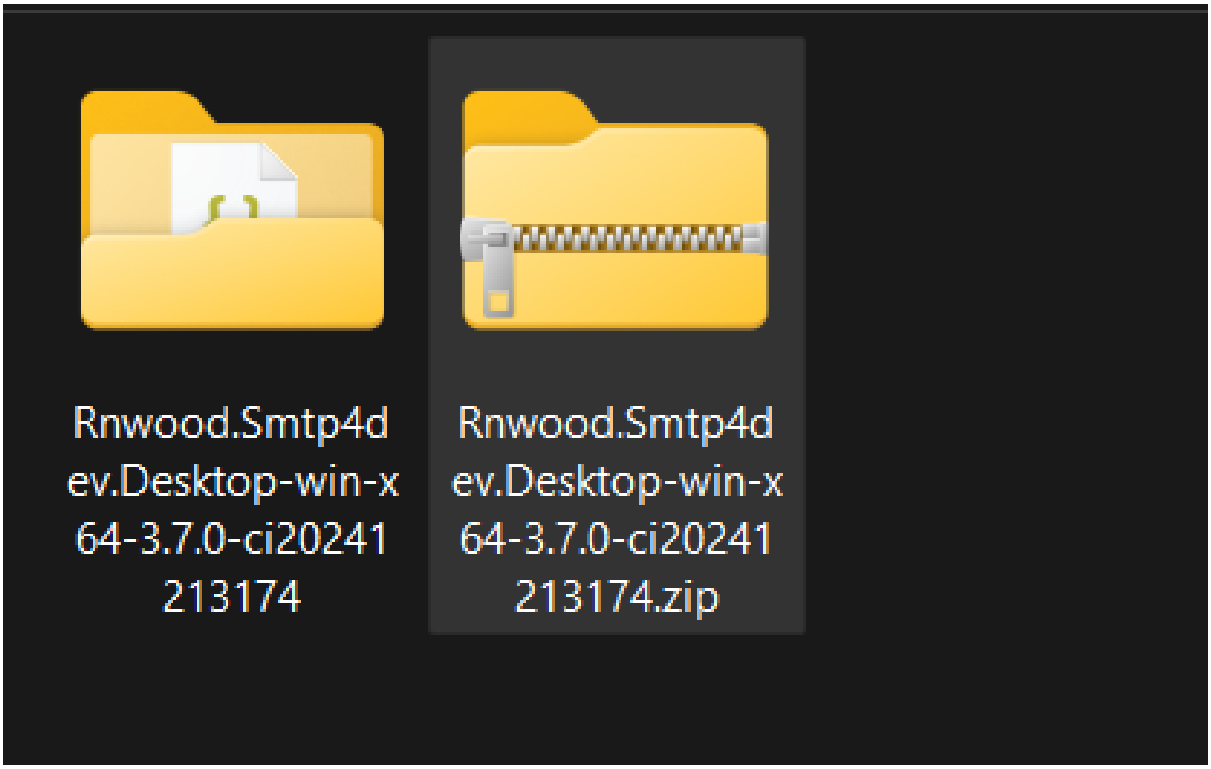
IMPLEMENTATION AND RESULTS:

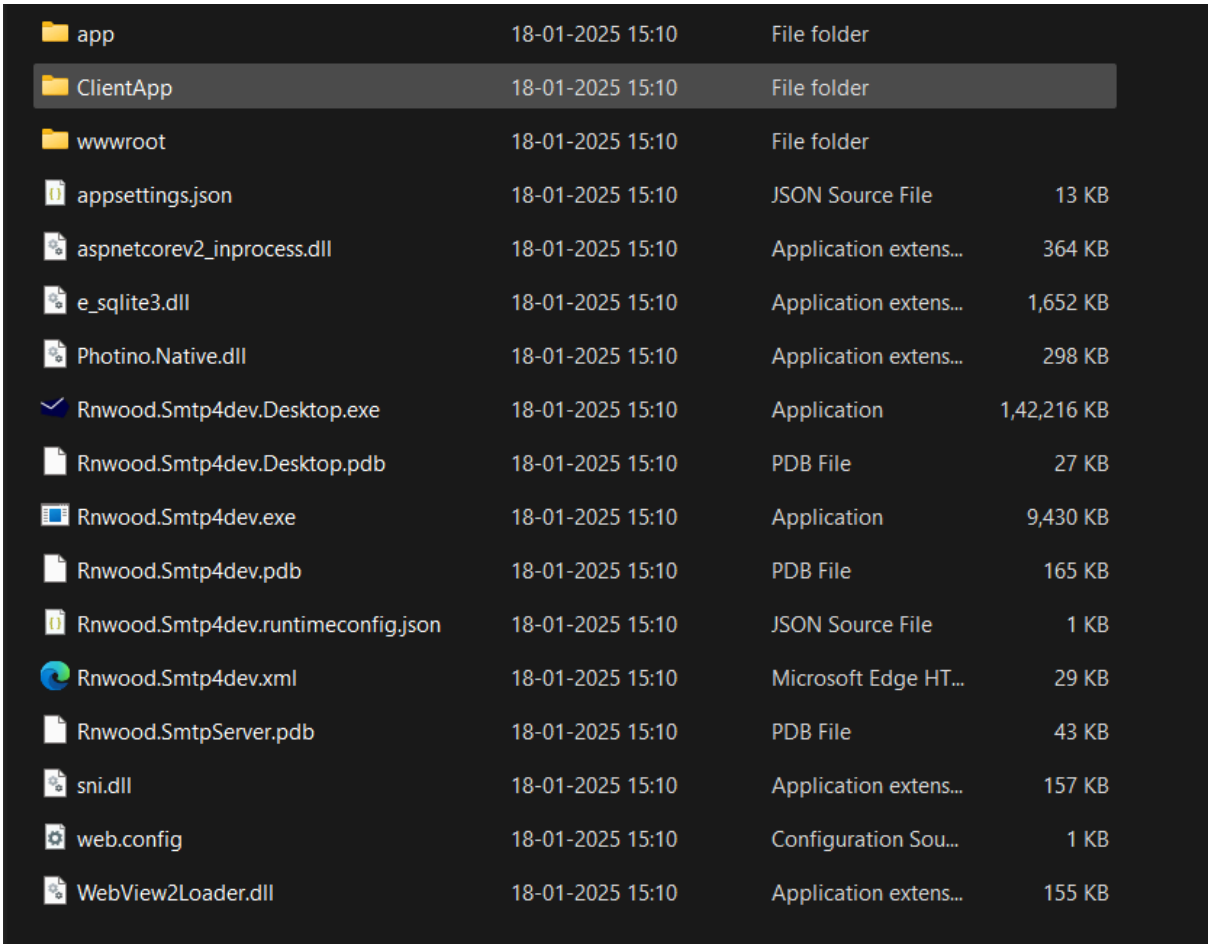
Step 1: Setup smtp4dev

Why smtp4dev? because its ethical and only operates on our local network.

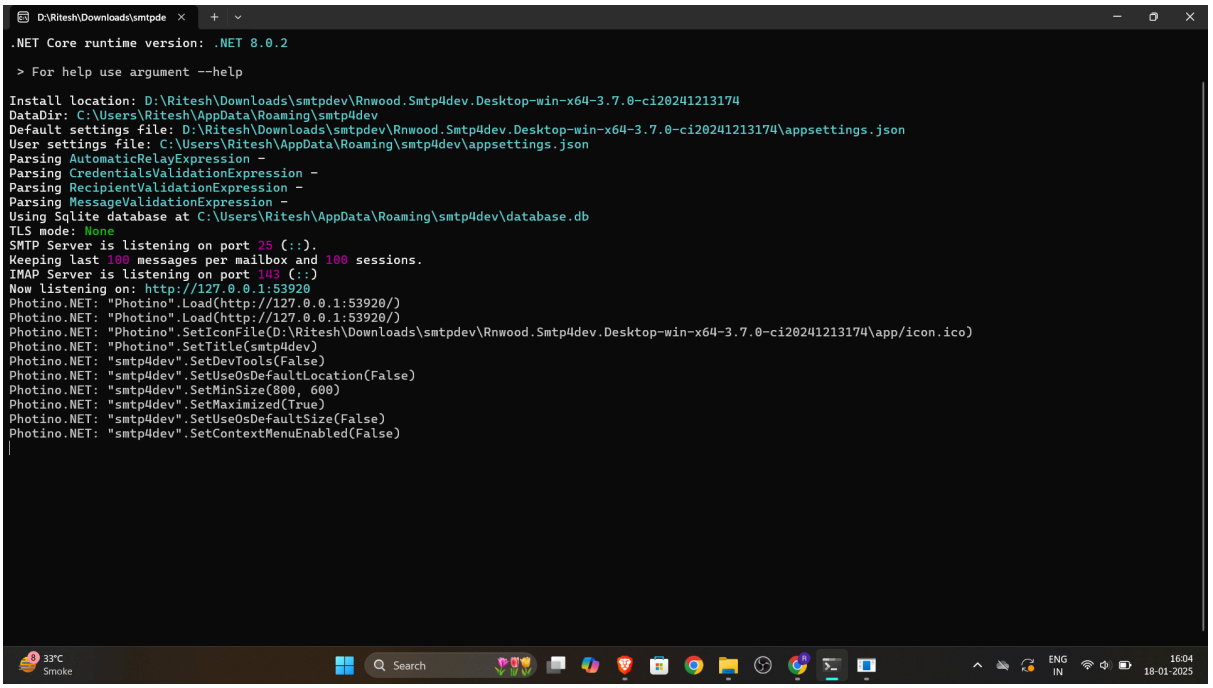
https://github.com/rnwood/smtp4dev/releases

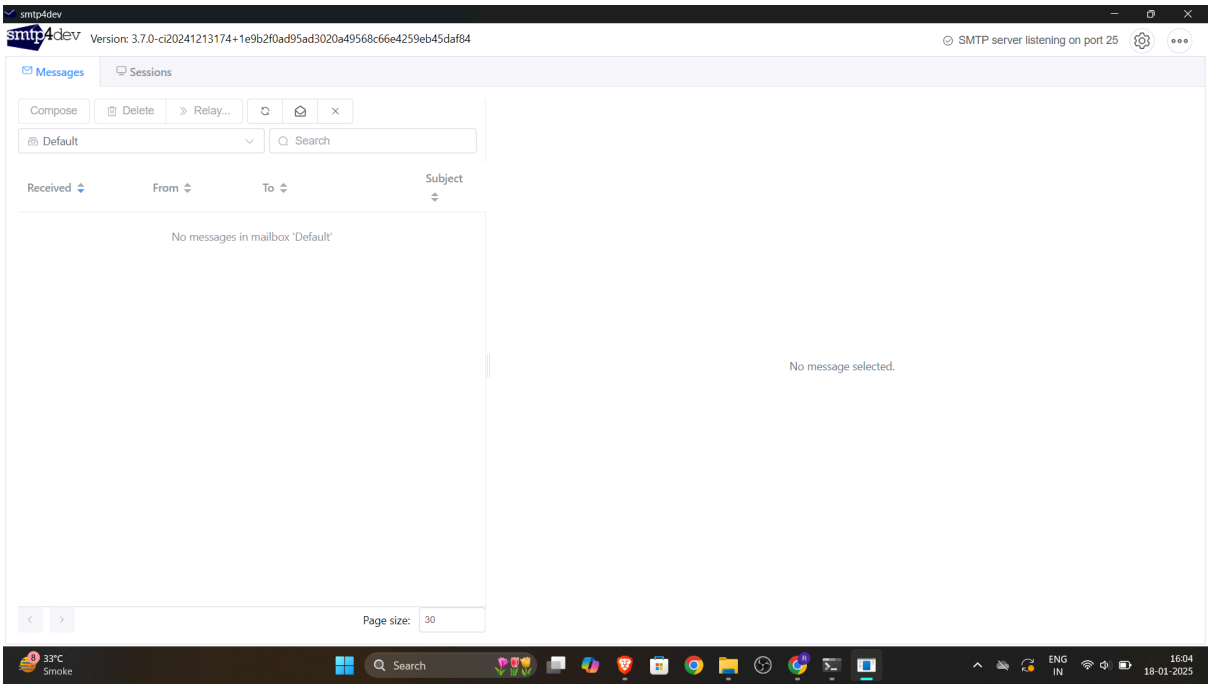



Rnwood.Smtp4dev.Desktop-win-x64-3.7.0-ci20241213174
Rnwood.Smtp4dev.Desktop-win-x64-3.7.0-ci20241213174.zip


app 18-01-2025 15:10 File folder
ClientApp 18-01-2025 15:10 File folder
wwwroot 18-01-2025 15:10 File folder
appsettings.json 18-01-2025 15:10 JSON Source File 13 KB
aspnetcorev2_inprocess.dll 18-01-2025 15:10 Application extens... 364 KB
e_sqlite3.dll 18-01-2025 15:10 Application extens... 1,652 KB
Photino.Native.dll 18-01-2025 15:10 Application extens... 298 KB
Rnwood.Smtp4dev.Desktop.exe 18-01-2025 15:10 Application 1,42,216 KB
Rnwood.Smtp4dev.Desktop.pdb 18-01-2025 15:10 PDB File 27 KB
Rnwood.Smtp4dev.exe 18-01-2025 15:10 Application 9,430 KB
Rnwood.Smtp4dev.pdb 18-01-2025 15:10 PDB File 165 KB
Rnwood.Smtp4dev.runtimeconfig.json 18-01-2025 15:10 JSON Source File 1 KB
Rnwood.Smtp4dev.xml 18-01-2025 15:10 Microsoft Edge HT... 29 KB
Rnwood.SmtpServer.pdb 18-01-2025 15:10 PDB File 43 KB
sni.dll 18-01-2025 15:10 Application extens... 157 KB
web.config 18-01-2025 15:10 Configuration Sou... 1 KB
WebView2Loader.dll 18-01-2025 15:10 Application extens... 155 KB

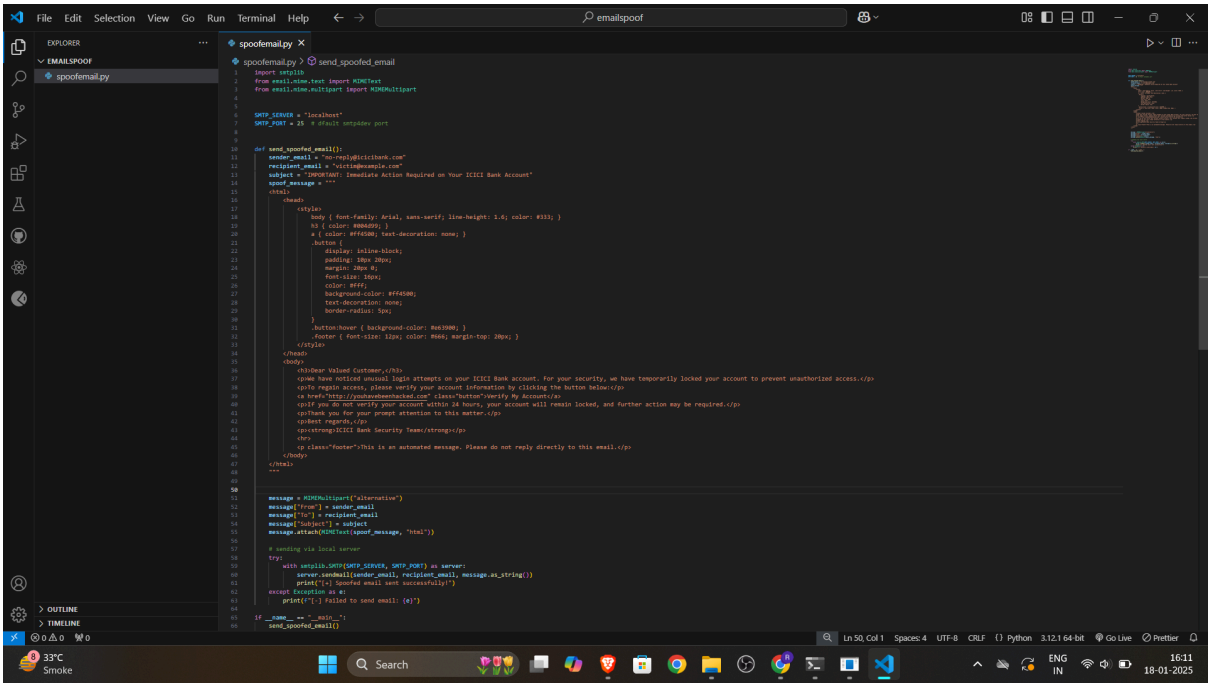
Step 2 : Run the Desktop executable file

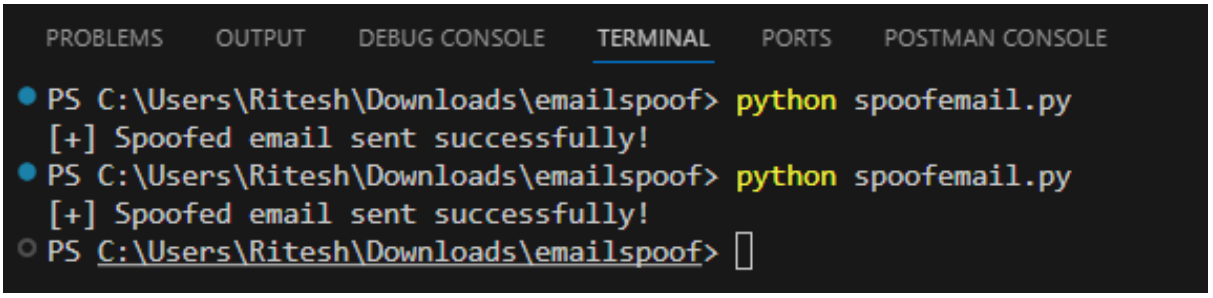




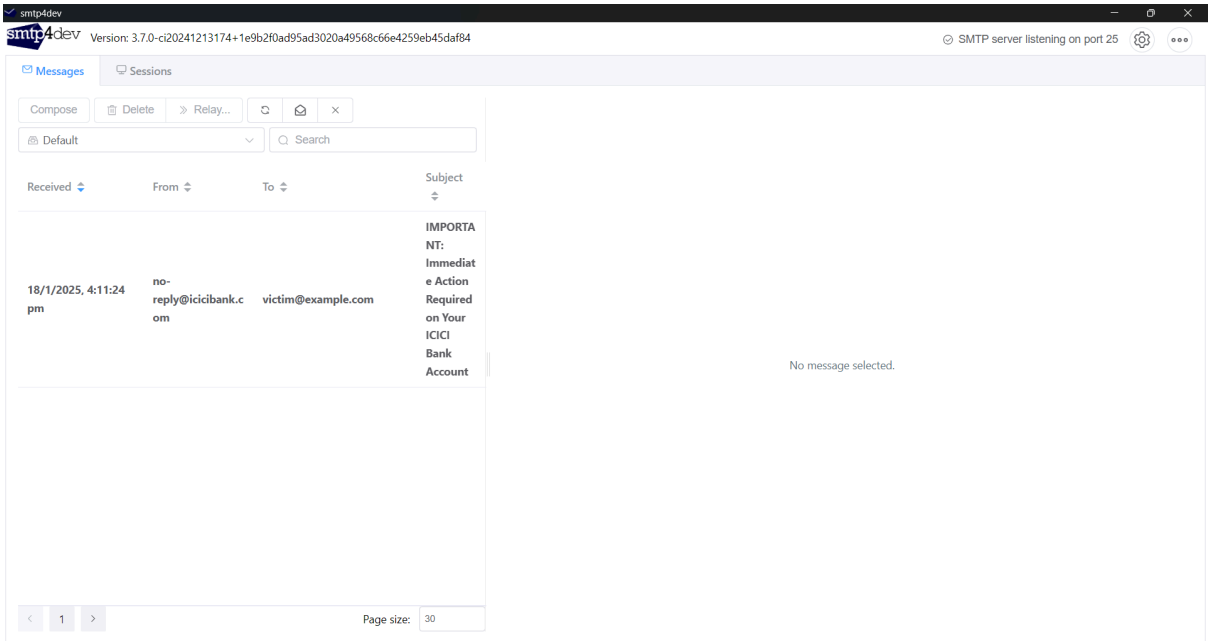
Step 3: Writing the Python Script to Send a Phishing Email

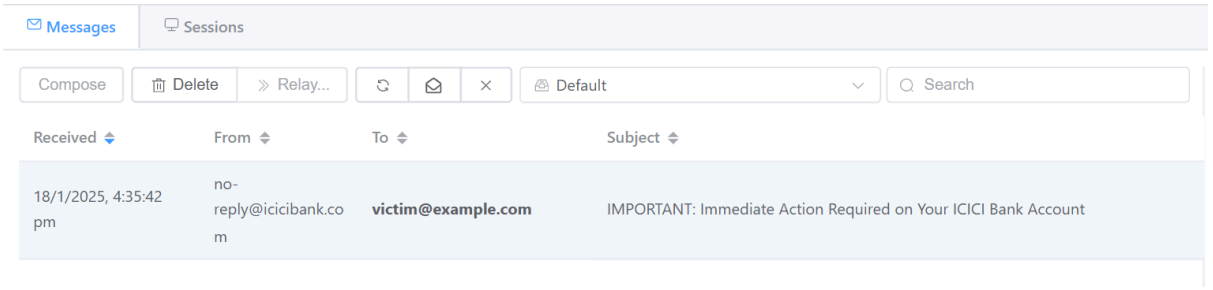
```
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart


SMTP_SERVER = "localhost"
SMTP_PORT = 25  # dfault smtp4dev port


def send_spoofed_email():
    sender_email = "no-reply@icicibank.com"
    recipient_email = "victim@example.com"
    subject = "IMPORTANT: Immediate Action Required on Your ICICI Bank Account"
    spoof_message = """
   <html>
        <head>
            <style>
                body { font-family: Arial, sans-serif; line-height: 1.6; color: #333; }
                h3 { color: #004d99; }
                a { color: #ff4500; text-decoration: none; }
                .button {
                    display: inline-block;
                    padding: 10px 20px;
                    margin: 20px 0;
                    font-size: 16px;
                    color: #fff;
                    background-color: #ff4500;
                    text-decoration: none;
                    border-radius: 5px;
                }
                .button:hover { background-color: #e63900; }
                .footer { font-size: 12px; color: #666; margin-top: 20px; }
            </style>
        </head>
        <body>
            <div style="text-align: center; margin-bottom: 20px;">
                <img src="https://getvectorlogo.com/wp-content/uploads/2018/12/icici-bank-vector-logo.png" alt="ICICI Bank Logo" width="200">
            </div>
            <h3>Dear Valued Customer,</h3>
               <p>We have noticed unusual login attempts on your ICICI Bank account. For your security, we have temporarily locked your account to prevent unauthorized
access.</p>
            <p>To regain access, please verify your account information by clicking the button below:</p>
            <a href="https://hackertroll.com" class="button">Verify My Account</a>
            <p>If you do not verify your account within 24 hours, your account will remain locked, and further action may be required.</p>
            <p>Thank you for your prompt attention to this matter.</p>
            <p>Best regards,</p>
            <p><strong>ICICI Bank Security Team</strong></p>
            <hr>
            <p class="footer">This is an automated message. Please do not reply directly to this email.</p>
        </body>
    </html>
    """


    message = MIMEMultipart("alternative")
    message["From"] = sender_email
    message["To"] = recipient_email
    message["Subject"] = subject
    message.attach(MIMEText(spoof_message, "html"))

    # sending via local server
    try:
        with smtplib.SMTP(SMTP_SERVER, SMTP_PORT) as server:
            server.sendmail(sender_email, recipient_email, message.as_string())
            print("[+] Spoofed email sent successfully!")
    except Exception as e:
        print(f"[-] Failed to send email: {e}")

if __name__ == "__main__":
    send_spoofed_email()
```

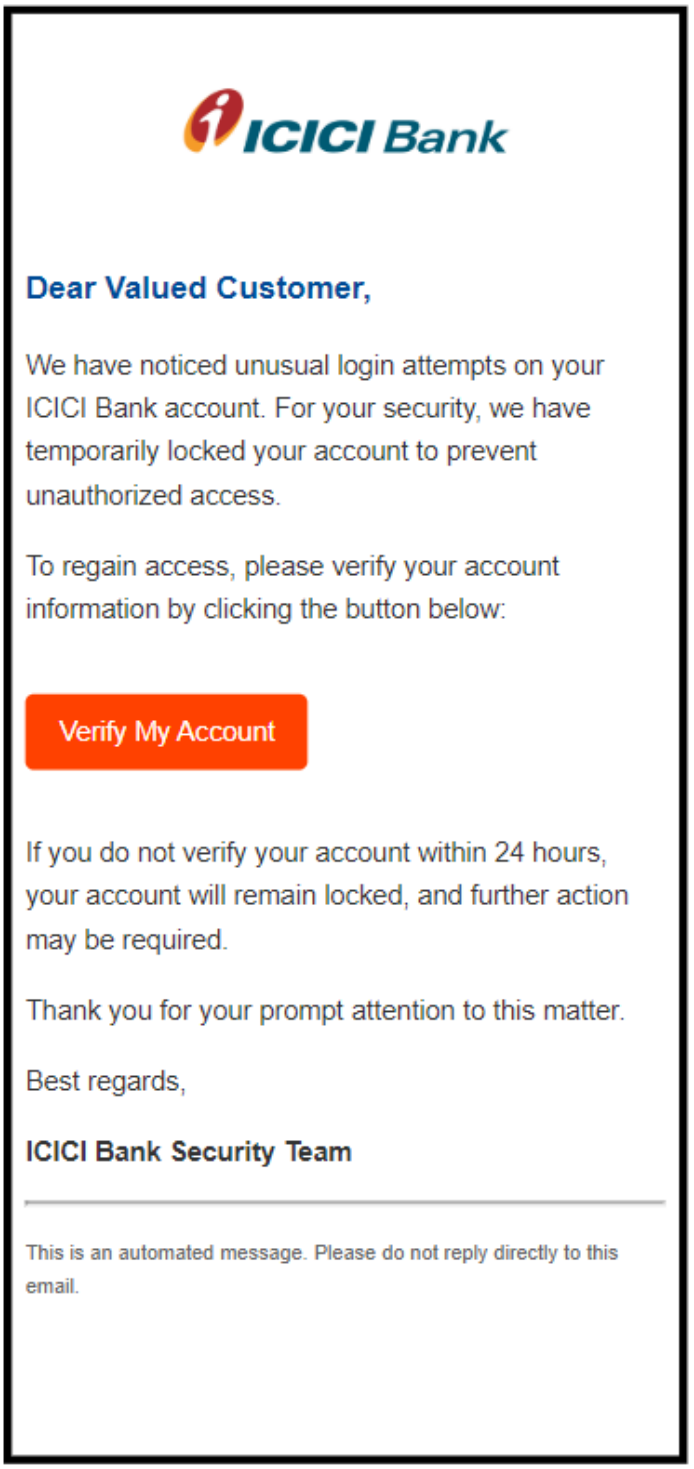




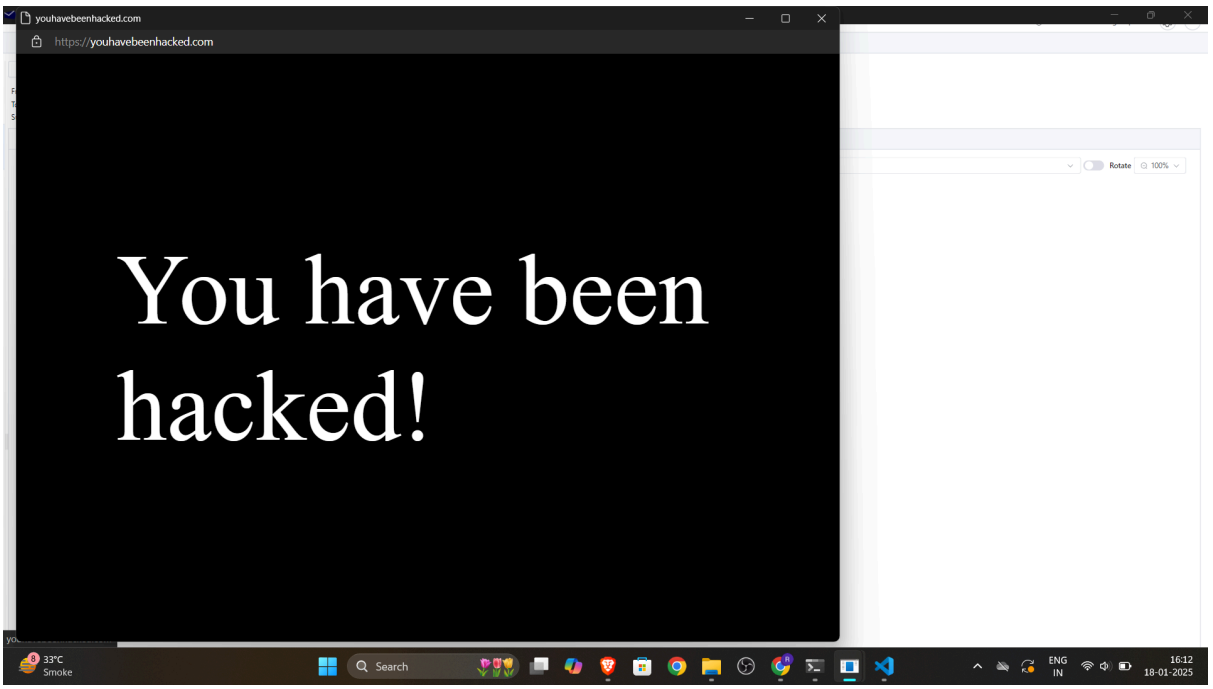
Now, if we check our inbox an email has been received from the email-ID of **no-reply@icicibank.com**


smtp4dev
Version: 3.7.0-ci20241213174+1e9b2f0ad95ad3020a49568c66e4259eb45daf84
SMTP server listening on port 25
Messages
Sessions
Compose
Delete
Relay...
Default
Search
Received
From
To
Subject
18/1/2025, 4:11:24 pm
no-reply@icicibank.com
victim@example.com
IMPORTANT: Immediate Action Required on Your ICICI Bank Account
No message selected.
1
Page size: 30


Messages
Sessions
Compose
Delete
Relay...
Default
Search
Received
From
To
Subject
18/1/2025, 4:35:42 pm
no-reply@icicibank.com
victim@example.com
IMPORTANT: Immediate Action Required on Your ICICI Bank Account



The link/href could be used to lead the user to a phishing website, or to upload malware onto their device !



Outcomes: CO1: Realize that premise of vulnerability analysis and penetration testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how phishing attacks exploit trust and urgency to trick individuals into revealing sensitive information. I gained practical insights into creating and detecting phishing emails using ethical tools like smtp4dev, enhancing my understanding of how attackers craft convincing scams. This hands-on experience emphasized the importance of proactive measures, such as recognizing phishing attempts and leveraging security practices, to mitigate risks in real-world scenarios.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

https://en.wikipedia.org/wiki/Phishing

https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44