**✅ Task 2: Analyze a Phishing Email Sample**

**🎯 Objective**

Identify phishing characteristics in a suspicious email sample.

**🧰 Tools Required**

| **Tool** | **Installed By Default?** | **Install Command (if needed)** |
| --- | --- | --- |
| nano, cat, grep | Yes | — |
| whois, curl | No | sudo apt install whois curl -y |
| gedit | No (GUI editor) | sudo apt install gedit -y |
| firefox | Yes | — |

**📁 Step-by-Step Guide with Example**

**🔹 Step 1: Obtain a Sample Phishing Email**

**✅ Option A: Download from a trusted source**

bash

Copy code

mkdir phishing-analysis

cd phishing-analysis

wget https://www.malware-traffic-analysis.net/2021/08/25/2021-08-25-eml-sample.eml -O sample.eml

**✅ Option B: Paste content manually**

bash

Copy code

nano sample.txt

# Paste the phishing email content here and save with Ctrl + O → Enter → Ctrl + X

📷 *Screenshot Example:*

nano sample.txt window showing pasted phishing email.

**🔹 Step 2: Check the Sender’s Email Address**

bash

Copy code

grep -i "From:" sample.txt

📷 *Screenshot Example:*

Terminal showing:  
From: "Apple Support" <support@apple.account-security.com>

⚠️ **Red Flag:** Domain is not @apple.com

**🔹 Step 3: Analyze Email Headers for Spoofing**

**Extract headers:**

bash

Copy code

grep -E "From:|To:|Subject:|Received:|Return-Path:" sample.txt

📷 *Screenshot Example:*

Terminal showing header lines: Return-Path:, Received:, etc.

**Analyze headers online:**

1. Open Firefox:

bash

Copy code

firefox https://mxtoolbox.com/EmailHeaders.aspx &

1. Paste the headers to analyze sender IP, SPF, DKIM, DMARC.

📷 *Screenshot Example:*

Browser showing the MxToolbox email header analyzer result with flags.

**🔹 Step 4: Identify Suspicious Links or Attachments**

bash

Copy code

grep -Eo "(http|https)://[^ \"']+" sample.txt

📷 *Screenshot Example:*

http://apple-login.security-check.net ← clearly suspicious

Check domain registration:

bash

Copy code

whois apple-login.security-check.net

📷 *Screenshot Example:*

Whois shows the domain is **recently registered** and has no link to Apple.

**🔹 Step 5: Find Urgent or Threatening Language**

bash

Copy code

grep -iE "urgent|immediately|suspend|verify|account" sample.txt

📷 *Screenshot Example:*

Terminal showing: “Your account has been suspended. Please verify now!”

**🔹 Step 6: Check for Mismatched URLs**

This is **manual**. In HTML emails, this might appear as:

html

Copy code

<a href="http://phishing-site.com">https://apple.com</a>

📷 *Screenshot Example:*

Email content shows "Click here to verify" with a fake link

**🔹 Step 7: Look for Grammar or Spelling Errors**

Open in a text editor:

bash

Copy code

gedit sample.txt &

📷 *Screenshot Example:*

Text: "Please confrim your pasword immidiately"

⚠️ Bad grammar and spelling – another phishing sign.

**📝 Step 8: Create the Phishing Report**

bash

Copy code

nano phishing-report.txt

**📄 Sample Report Content:**

txt

Copy code

# Phishing Email Analysis Report

\*\*Sample File:\*\* sample.txt

1. \*\*Spoofed Sender:\*\*

- From: Apple Support <support@apple.account-security.com>

- Domain not genuine.

2. \*\*Header Discrepancies:\*\*

- Return-path and "From" mismatch.

- Suspicious Received path.

3. \*\*Suspicious Links:\*\*

- http://apple-login.security-check.net

- Whois shows it's not an official Apple domain.

4. \*\*Threatening Language:\*\*

- “Your account has been suspended. Please verify now!”

5. \*\*Mismatched URLs:\*\*

- Link text and real link differ.

6. \*\*Spelling Errors:\*\*

- “confrim your pasword”

\*\*Conclusion:\*\*

This email contains multiple phishing indicators. It is a phishing attempt and should be reported or deleted.

📷 *Screenshot Example:*

Terminal with phishing-report.txt open in nano

**📌 Summary Table**

| **Check** | **Tool/Command** |
| --- | --- |
| Download email | wget, nano |
| Sender address | grep "From:" |
| Headers | grep, firefox + MxToolbox |
| Suspicious links | grep -Eo, whois |
| Threat language | grep -iE |
| Grammar errors | gedit |
| Final report | nano phishing-report.txt |