Cybersecurity Internship

Task 2: Phishing Email Analysis

Objective:

- To analyse a sample phishing email and identify key phishing indicators such as spoofed sender address, malicious links, and social engineering techniques used by attackers.

Tools Used:

- Browser (for hovering over links),
- MxToolbox Email Header Analyser,
- Text Editor
- OS -windows

Steps Performed:

1. Obtained a sample phishing email from online sources.
2. Analyzed sender email address for spoofing (e.g., misspelled domain like secure-paypa1.com).
3. Checked headers using MxToolbox to identify mismatch in sending server and SPF failure.
4. Inspected hyperlinks by hovering over them to find mismatches (e.g., PayPal link pointing to a fake domain).
5. Reviewed the message content for urgency, threats, and spelling/grammar issues.
6. Summarized the phishing indicators in a structured report

Findings:

✓ Spoofed email domain
✓ Suspicious link with fake login page
✓ Urgent and threatening message tone
✓ No personalization
✓ Spelling and formatting errors

Conclusion:

- This email is a phishing attempt aiming to steal user credentials using spoofed domains and social engineering. The analysis improved understanding of phishing tactics and threat detection.