Task 2 Assessment Report - Phishing Campaign Analysis

1. Task Overview

This report summarizes the investigation of a large-scale phishing campaign using malicious emails and URLs. Tools and methods learned in the lectures were applied to uncover the campaign's organization.

2. Evidence Collected

Emails: Suspicious emails collected from lab environment.

Attachments: Update365.zip phishing kit.

Malicious URLs: Example: hxxp\://kennaroads.buzz/data/Update365/...

3. Email Analysis

Inspect sender addresses, timestamps, and headers.

SPF/DKIM/DMARC checks for spoofing.

Observed patterns: similar subject lines, repeated domains.

4. Phishing URL Analysis.

URLs analyzed safely.

Redirection chains confirmed phishing behavior.

Domain registration and SSL checks indicated fraudulent setup.

5. Phishing Kit Inspection

A, Extracted Update365.zip safely.

office365/ folder contains scripts for credential harvesting.

B, Hidden flag identified: THM{pL4y_w1Th_tH3_URL}

C, File hash example: sha256sum Update365.zip = ba3c15267393419eb08c7b2652b8b6b39b406ef300ae8a18fee4d16b19ac9686

6. Indicators of Compromise (IOCs)

Type	Value
Malicious URL	hxxp\://kennaroads.buzz/...
File Hash:	ba3c15267393419eb08c7b2652b8b6b39b406ef300ae8a18fee4d16b19ac9686

Phishing Kit Update365.zip / office365 folder

Victim Email zoe.duncan@swiftspend.finance

mailto:zoe.duncan@swiftspend.finance

E.t.c

7. Conclusion

The phishing campaign was organized using mass email distribution, malicious URLs, and a credential-harvesting kit (Update365). Analysis confirms it is a large-scale, structured attack.