CyberDefenders HawkEye Lab – Blue Team Analysis Report

Student Name: Suhas
Role: Blue Team Analyst (Intern)
Platform: CyberDefenders
Challenge Name: HawkEye

1. Objective

The objective of the HawkEye lab is to analyze a suspicious phishing email and identify malicious indicators using blue team techniques.

2. Tools Used

CyberDefenders Lab Environment, Email Header Analyzer, VirusTotal, WHOIS Lookup, URL Reputation Tools, Base64 Decoder.

3. Step-by-Step Analysis

Step 1: Accessed the HawkEye challenge and downloaded the email evidence file.
Step 2: Analyzed email headers to identify spoofing, sender IP, and authentication failures.
Step 3: Examined the email body and identified phishing indicators and suspicious URLs.
Step 4: Investigated the URL using VirusTotal and confirmed malicious behavior.
Step 5: Performed WHOIS lookup on the domain to verify registration details.
Step 6: Decoded Base64 encoded content to uncover hidden redirection links.

4. Indicators of Compromise

Malicious URL, Suspicious Sender IP, Fake Domain, Encoded Phishing Link.

5. MITRE ATT&CK; Mapping

T1566.001 – Phishing: Spearphishing Link
T1204.002 – User Execution: Malicious Link

6. Conclusion

The HawkEye lab provided hands-on experience in identifying phishing attacks using blue team methodologies and threat intelligence tools.

Submission Statement

This report is submitted as part of my cybersecurity internship learning activities.