REPORT 1: Red Team Report – HawkEye Lab

Student Name: Suhas
Role: Red Team Intern

Objective

Simulate a phishing attack to demonstrate attacker techniques such as spoofed emails, malicious URLs, and evasion strategies.

Attack Methodology

Reconnaissance, phishing email crafting, payload delivery using encoded URLs, and domain spoofing.

MITRE ATT&CK;

T1566.001 – Phishing
T1027 – Obfuscated Files/Information

Conclusion

The lab demonstrates how attackers exploit human trust through phishing campaigns.

REPORT 2: Blue Team Report – HawkEye Lab

Student Name: Suhas
Role: Blue Team Intern

Objective

Detect, analyze, and mitigate phishing attacks using email forensics and threat intelligence.

Defense Workflow

Email header analysis, URL inspection, decoding malicious content, IOC blocking.

MITRE ATT&CK;

T1566 – Phishing Detection

Conclusion

The phishing email was successfully identified and neutralized.

REPORT 3: Purple Team Report – HawkEye Lab

Student Name: Suhas
Role: Purple Team Intern

Objective

Bridge red and blue team findings to improve detection and response capabilities.

Key Findings

Effective phishing detection relies on collaboration between attack simulation and defense analysis.

Recommendations

Improve DMARC enforcement, user awareness, and SIEM alerting.

Conclusion

Purple Team collaboration enhances organizational security posture.