CYBER SECURITY INTERNSHIP
Task 11: Interview Questions & Answers
Phishing Attack Simulation & Detection

Tool Used

GoPhish was used on Kali Linux to simulate phishing attacks. Mailtrap was used as a sandbox SMTP server for safe email testing.

Objective

To understand phishing attacks by performing a controlled phishing simulation and analyzing detection techniques, user behavior, and prevention methods.

Working & Steps

• Studied phishing attack concepts and social engineering techniques.

• Accessed and configured GoPhish on Kali Linux.

• Created a phishing email template to simulate an account verification alert.

• Configured a fake login landing page for credential capture.

• Configured SMTP using Mailtrap for safe email delivery.

• Launched a phishing campaign using test email accounts.

• Tracked email delivery, link clicks, and credential submissions using GoPhish.

• Reviewed campaign analytics and user interaction results.

• Documented phishing indicators and prevention strategies.

Phishing Red Flags Identified

• Urgent or threatening language used to pressure users

• Generic greetings instead of personalized messages

• Suspicious or unexpected hyperlinks

• Requests for login credentials or sensitive information

• Unverified or spoofed sender addresses

Prevention Methods

• Regular security awareness training for users

• Email filtering and spam protection systems

• Verifying sender email addresses and URLs

• Avoiding clicking unknown or suspicious links

• Using multi-factor authentication (MFA)

• Reporting phishing emails to security teams

Interview Questions & Answers

What is phishing?

Phishing is a social engineering attack in which attackers impersonate legitimate entities to trick users into revealing sensitive information such as usernames, passwords, or financial details.

What are the types of phishing?

Types of phishing include email phishing, spear phishing (targeted attacks), whaling (targeting executives), smishing (SMS phishing), and vishing (voice phishing).

How can phishing be detected?

Phishing can be detected by identifying suspicious links, urgent or threatening language, unexpected requests for sensitive information, and verifying sender authenticity.

Why is phishing dangerous?

Phishing is dangerous because it can result in credential theft, financial fraud, identity theft, unauthorized system access, and data breaches.

What are the prevention methods for phishing?

Phishing can be prevented through user awareness training, email security tools, multi-factor authentication (MFA), careful link verification, and proper reporting mechanisms.

Final Outcome

This task improved understanding of phishing attacks and enhanced awareness of social engineering techniques, detection strategies, and prevention methods.