Phishing Awareness

Task: Conduct a simulated phishing campaign and provide training on identifying phishing emails.

What is Phishing?

Phishing attacks deceive users into disclosing sensitive information, such as login credentials and financial details, by masquerading as a trustworthy entity. Training employees to recognize and report phishing attempts strengthens an organization's security posture.

Steps to Conduct a Simulated Phishing Campaign

Select a Phishing Simulation Tool

Use tools like GoPhish, PhishMe, or KnowBe4 to create and manage phishing simulations.
Design Realistic Phishing Emails

Mimic common phishing attempts (e.g., fake password reset requests, invoice fraud, or impersonation emails).
Include subtle red flags (e.g., misspelled URLs, urgency in tone).
Launch the Simulation

Send phishing emails to a test group of employees or users.
Monitor who interacts with the fake phishing links.
Analyze the Results

Identify how many users clicked the link or entered credentials.
Gather data on who fell for the phishing attempt.
Conduct Phishing Awareness Training

Educate employees on phishing tactics and warning signs.
Explain the importance of verifying email senders and avoiding suspicious links.
Encourage reporting suspicious emails to IT/security teams.
Re-test Regularly

Conduct periodic phishing simulations to measure improvement.
Reinforce training with updated phishing scenarios.

Phishing Simulation Tools:

GoPhish
KnowBe4
PhishMe