PLAN D'ATTAQUE PHISHING

MASTER CYBERSÉCURITÉ - UNIVERSITÉ DE CORSE

IDENTIFICATION DES CIBLES

- Population cible : Étudiants et personnel universitaire
- Type d'attaque : Phishing ciblé (spear phishing)
- Collecte emails : Scraping de l'annuaire universitaire
- Utilisation des comptes inactifs pour accès aux listes de diffusion

SCÉNARIO D'ATTAQUE

- Contexte : Intégration d'un nouvel assistant IA dans l'ENT
- Email officiel : Annonce : un nouvel assisant dans votre espace
- Page de connexion : Clone de l'interface ENT

SOLUTIONS TECHNIQUES

- Mailing : SMTP via Gmail + SendGrid
- Domaine : services.etudiant.univ.corse@gmail.com
- Site clone : Reproduction exacte de l'ENT
- Système de logging sécurisé

MESURES ÉTHIQUES

- Destruction immédiate des données après analyse
- Email de débriefing post-attaque
- Respect RGPD et confidentialité
- But pédagogique uniquement

ÉVALUATION ET MÉTRIQUES

- Taux de clics sur les liens
- Taux de conversion (identifiants saisis)
- Temps de réaction du service informatique
- Analyse démographique des résultats

PLANIFICATION

- Phase 1 : Développement infrastructure (2 semaines)
- Phase 2 : Tests et validation (1 semaine)
- Phase 3 : Exécution de l'attaque (1 jour)
- Phase 4 : Analyse et rapport (1 semaine)