Sujet de Travaux Pratiques : Application des Concepts de Cybersécurité

Soufian Ben Amor et William Jalby (LI-PaRAD) *

Introduction

Ce TP a pour objectif de vous permettre de mettre en pratique les concepts de cybersécurité abordés lors du cours. Vous apprendrez à identifier des menaces courantes, créer et gérer des mots de passe sécurisés, et protéger vos communications électroniques contre le phishing et les spams.
Remarque : pour certains exercices nécessitant une adresse mail valide, vous pouvez utiliser une adresse mail jetable, que vous pouvez créer pour des besoins ponctuels à l'dresse suivante : https://temp-mail.org

Instructions Générales

- Lisez attentivement chaque section avant de commencer.
- Utilisez uniquement les plateformes en ligne recommandées (aucune installation nécessaire).
- Travaillez individuellement ou en petits groupes selon les consignes données.
- Prenez note de vos observations et réponses pour les discussions finales.

Ressources Utiles

- Guides ANSSI : https://www.ssi.gouv.fr/guide/
- Documentation RGPD : https://www.cnil.fr/fr/me-mettre-en-conformite/rgpd-par-ou-commencer
- PhishTank : https://www.phishtank.com/
- Password Generator : https://passwordsgenerator.net/
- How Secure Is My Password : https://howsecureismypassword.net/
- Bitwarden : https://bitwarden.com
- Phishing Quiz : https://phishingquiz.withgoogle.com/

Exercice 1 : Identifier les Menaces (30 minutes)

Objectif

Analyser des scénarios réalistes pour identifier des actions malveillantes potentielles et proposer des solutions.

Instructions

1. **Étude des Scénarios** : Examinez les deux scénarios ci-dessous et identifiez les risques associés. Proposez des solutions pour éviter ces menaces.

   Scénario 1 : E-mail Suspect

   Vous recevez un e-mail intitulé "Facture non payée" avec une pièce jointe nommée `facture.pdf`. L'expéditeur est `support@paiements-online.com`.

   Scénario 2 : Clé USB Trouvée

   Une clé USB inconnue est trouvée dans le bureau de votre service. Elle contient plusieurs fichiers intitulés `confidentiel.docx` et `rapport-financier.xlsx`.
2. **Discussion en Groupe** : Discutez avec vos camarades pour partager vos analyses. Identifiez ensemble les bonnes pratiques à adopter dans chaque cas.
3. **Simulation sur PhishTank** : Accédez à PhishTank. Explorez la base de données d'e-mails de phishing signalés. Sélectionnez un exemple d'email frauduleux et analysez ses caractéristiques (adresse e-mail, contenu, liens).

Exercice 2 : Création et Gestion de Mots de Passe (30 minutes)

Objectif

Créer des mots de passe forts et apprendre à les gérer efficacement à l'aide d'un gestionnaire de mots de passe en ligne.

Instructions

1. **Création de Mots de Passe Forts** : Utilisez l'outil en ligne Password Generator pour générer trois mots de passe complexes. Chaque mot de passe doit contenir au moins :
   — 12 caractères.
   — Des lettres majuscules et minuscules.
   — Des chiffres.
   — Des caractères spéciaux (`!`, `@`, `#`, etc.).

2. **Test de Force de Mot de Passe** : Testez chaque mot de passe sur How Secure Is My Password. Notez combien de temps chaque mot de passe résisterait à une attaque brute force.
3. **Configuration d'un Gestionnaire de Mots de Passe** : Inscrivez-vous sur Bitwarden (gratuit). Ajoutez vos trois mots de passe générés dans le gestionnaire. Activez la double authentification (2FA) pour renforcer la sécurité de votre compte.
4. **Réflexion** : Quelles sont les principales avantages d'utiliser un gestionnaire de mots de passe ? Pourquoi est-il important de ne pas réutiliser les mêmes mots de passe ?

Exercice 3 : Gestion de la Messagerie et des Spams (30 minutes)

Objectif

Apprendre à détecter les e-mails de phishing et à configurer des règles pour trier efficacement les spams.

Instructions

1. **Analyse de Faux E-mails de Phishing** : Consultez les exemples d'e-mails de phishing disponibles sur Phishing Quiz. Répondez aux questions pour tester vos compétences en identification de phishing. Notez les indices qui vous ont permis de détecter les e-mails frauduleux (ex. adresse e-mail incorrecte, orthographe, demande urgente).
2. **Configuration de Règles Anti-Spam** : Connectez-vous à votre compte Gmail. Créez une règle pour marquer comme spam tous les e-mails provenant d'adresses contenant le mot "remboursement".
   — Aller à **Paramètres** > **Filtres et blocage des expéditeurs** > **Créer un filtre**.
   — Entrez `remboursement` dans le champ "De" ou "Objet".
   — Choisissez l'action "Marquer comme spam".
3. **Atelier Pratique** : Échangez avec vos camarades pour discuter des meilleures stratégies pour éviter les phishing et les spams. Partagez vos règles anti-spam et expliquez pourquoi elles sont efficaces.

Conclusion et Questions de Réflexion

À la fin des exercices, participez à une discussion collective pour répondre aux questions suivantes :

1. Quels sont les principaux risques en cybersécurité dans le secteur de la santé ?
2. Comment pouvez-vous protéger vos données personnelles et celles de vos patients ?
3. Quelle importance accordez-vous à la formation continue en cybersécurité ?