**GESTION DES RISQUES INFORMATIQUES**

**DESS en Technologie de l'Information**

**EXERCICES D’APPLICATION 1**

**Exercice 1**

1. **Associer la menace à sa description**

Associe chaque menace au bon exemple :

|  |  |
| --- | --- |
| **Menace** | **Exemple correspondant** |
| 1. Ransomware(B) | A. Un email prétend venir de ta banque pour voler tes identifiants. |
| 2. Phishing (A) | B. Un fichier infecté chiffre tes données et demande une rançon. |
| 3. DDoS (C) | C. Un pirate envoie des millions de requêtes pour saturer un site. |

1. **Choisir la bonne réponse**

Quelle est la meilleure manière d’éviter une attaque par **phishing** ?

A) Ouvrir tous les emails et vérifier si un lien semble intéressant.

1. Vérifier l’expéditeur et ne pas cliquer sur des liens suspects.
2. Partager ses identifiants avec un collègue pour qu’il vérifie.

**3. Trouver l’intrus**

Lequel de ces fichiers a le plus de chances d’être un **malware** ?

1. rapport\_financier.pdf
2. mise\_a\_jour\_systeme.exe
3. photo\_anniversaire.jpg

**Exercice 2**

1. **Identifier une attaque dans un scénario**

Un employé reçoit un email urgent :

*"Votre compte Microsoft est bloqué. Cliquez ici pour le débloquer."* Il clique et entre ses identifiants.

*Rep : Attaque par phishing*

1. **Trouver la faille de sécurité**

Un employé laisse son ordinateur allumé et déverrouillé en partant déjeuner. Son collègue en profite pour copier des fichiers confidentiels.

**Quelle erreur de sécurité a été commise ?**

Intrusion physique.

1. **Compléter la phrase**

Une attaque **DDoS** consiste à \_\_saturer un serveur d’\_\_\_\_\_\_\_\_\_\_\_\_ un site web en lui envoyant \_\_\_\_des multiples requêtes\_\_\_\_\_\_\_\_\_\_.

1. **Analyser un cas de ransomware**

Un utilisateur voit un message sur son écran :

*"Vos fichiers sont chiffrés ! Payez 500€ en Bitcoin pour les récupérer."*

➡️ **Que doit-il faire ?** (Choisir la meilleure réponse)

A) Payer la rançon immédiatement.

1. Débrancher son PC d’Internet et contacter un expert en cybersécurité.
2. Redémarrer son PC en espérant que tout revienne à la normale.

**Exercices 3**

1. **Analyse d’un email suspect**

Voici un email reçu :

**De :** support@paypal-secure.com

**Objet :** Problème de paiement !

Bonjour,

Nous avons détecté un problème avec votre compte PayPal. Cliquez sur ce lien pour le résoudre immédiatement : [www.paypal-verification.com](http://www.paypal-verification.com/)

Cordialement,

Service client PayPal

**Repérer 3 signes que cet email est un phishing.**

-A cause de l’adresse mail qui n’est correct pas.

-Qu’il va résoudre le problème dans l’immediaire.

-A Cause du lien

1. **Étude d’une faille logicielle**

Un logiciel bancaire a un bug : en tapant admin' OR '1'='1 dans le champ mot de passe, on accède au compte administrateur.

**Quelle faille est exploitée ici ?**

C’est une injection SQL qui permet de contourner l’authentification en modifiant la requête SQL.

1. **Étudier un cas d’intrusion physique**

Un pirate trouve un badge d’employé et entre dans une entreprise. Il accède à un serveur non surveillé et vole des fichiers.

➡️ **Quelle(s) mesure(s) auraient pu empêcher cela ?**

Rep : Installer des caméras de surveillance et interdire de rentrer dans les zones sensibles.

1. **Détection d’un malware dans un processus système**

Un administrateur système remarque qu’un processus inconnu, svchost\_fake.exe, consomme énormément de ressources CPU et envoie des requêtes vers une adresse IP suspecte.

➡️ **Quelle menace soupçonnes-tu ? Comment enquêter plus en détail ?**

**Rep : Cheval de Troie ou bodnet, on peut analyser les connexions réseau.**

1. **Identifier une attaque cachée**

Une entreprise reçoit des plaintes : plusieurs clients disent avoir reçu des factures étranges contenant un fichier .zip. À l’intérieur, un fichier facture.pdf.exe est présent.

**Quelle attaque est en cours ? Pourquoi ce fichier est suspect ?**

Rep : DDOS. Fixer les emails.

1. **Analyse d’une attaque DDoS**

Un site e-commerce subit une attaque et devient indisponible. L’administrateur réseau remarque une augmentation anormale des requêtes venant de milliers d’IP différentes.

➡️ **Quel type d’attaque est en cours ? Comment la bloquer ?**

Rep: DDOS,on peut utiliser un parefeu

1. **Étude d’un cas de phishing avancé**

Un PDG reçoit un email qui semble venir du directeur financier :

"Urgent ! Peux-tu virer 10 000 dollar au fournisseur X sur ce compte bancaire ?

C’est très important."

➡️ **Quel type d’attaque est-ce ? Comment l’éviter ?**

REP: Attaque par phishing

1. **Analyse d’une intrusion physique réussie**

Un employé oublie son badge dans un café. Un inconnu le ramasse, entre dans l’entreprise et accède aux salles serveurs.

**Quelles erreurs ont été commises ? Quelles mesures mettre en place ?**

Rep : Intrusion physique, désactiver la Badge

1. **Détection d’une exploitation de faille logicielle**

Un pirate découvre qu’un site web contient un champ de recherche vulnérable à une **injection SQL**. En tapant :

sql

CopierModifier ' OR '1'='1' --

Il accède aux données des utilisateurs.

**Quelle faille est exploitée ? Comment la corriger ?**

L’injection SQL. En utilisant des requêtes paramétrées.

1. **Identifier un ransomware dormant**

Un employé télécharge un fichier douteux mais ne remarque aucun effet immédiat.

Un mois plus tard, ses fichiers sont chiffrés et une demande de rançon apparaît.

**Pourquoi ce ransomware a-t-il attendu ? Comment prévenir ce genre d’attaque ?**

Rep : ransomware dormant, il faut analyser les fichiers suspect

1. **Détection d’un vol d’identifiants par keylogger**

Un employé remarque que ses mots de passe sont utilisés sans son consentement.

Après analyse, il découvre un processus caché enregistrant tout ce qu’il tape au clavier.

➡️ **Quel type de malware est utilisé ? Comment s’en protéger ?**

Rep: Keylogger

1. **Repérer une intrusion réseau suspecte**

Un administrateur voit des connexions étranges venant d’un port inhabituel (TCP 4444). Après analyse, il découvre un programme inconnu qui envoie des données vers l’extérieur.

➡️ **Quelle menace est en cours ? Quelle action prendre ?**

Rep: Cheval de troie, bloquer les addresses IP Sispects

1. **Étude d’un vol de données via USB**

Un employé malintentionné branche une clé USB et copie des documents confidentiels avant de quitter l’entreprise.

➡️ **Comment empêcher ce type d’attaque ?**

Rep : Désactiver les ports USB sur les machines sensibles.