|  |  |
| --- | --- |
| **Nom** | Nasredine |
| **Prénom** | Abdelli |
| **Promotion** | 2 MSIR |

Exercice 1

L’utilisation d’un ordinateur pour gérer un projet de fin d’étude a des nombreuse risques, comme :

* documents dommages dus à une coupure de courant, panne matérielle (disque dur), échec du système d’exploitation (Blue Screen of Death), infection par virus ou trojen (Clé usb infecter)
* les fichiers peuvent être volés, supprimés ou modifiés par un hacker

|  |  |
| --- | --- |
| **Objectifs** | **Confidentialité**  Protéger le dossier avec du cryptage par mot de passe à l'aide des outils inclus de OS (Windows encrypt) ou avec des logiciel tiers tel que 7-zip (encrypted archive) ou AxCrypt. |
| **Disponibilité**  Sauvegarder des copies sur un appareil comme un disque dur externe ou clé USB, aussi, l’utilisation des systèmes de sauvegarde en ligne (Dropbox, Google Drive, …), systèmes vcs «*version control system*» pour le code source de PFE (git, github, gitlab…). |
| **Intégrité**  l’utilisation des checksums qui garantit que les fichiers ne sont pas modifiés. |
| **Non répudiation**  Signature numérique |
| **Authentification**  Protéger le compte Windows à l’aide d’un nom d’utilisateur et un mot de passe |

Les pertes possibles peuvent être : (Menace a Confidentialité)

* les informations du client de cette Bank (username, password «si elle est en clair » …)
* les transactions effectuées par le client (montant, crédit)

Exercice 2

|  |  |
| --- | --- |
| ***Assets*** | serveur Web, site Web de l’organisation |
| ***Risks*** | serveur deviant inaccessible, diffusion des informations des clients, lien de site renvoi à un autre site |
| ***Threat*** | spyware, ransomeware, un compétiteur malhonnête, |
| ***Vulnerability*** | Porte ouverte, Antivirus n’est pas à jour, employé insatisfait |

Exercice 3

|  |  |
| --- | --- |
| **Mot** | **Définition** |
| **Virus** | logiciel malveillant « malware »  conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber le fonctionnement de l'ordinateur infecté. |
| **RootKit** | collection des logiciel malveillants pour faire access a des parties de ordinateur / logiciels non authorisé ou de caché sa présence ou la présence d’autre logiciel |
| **Ver** | malware comme les virus qui se reproduire sans besoin d’un logiciel hôte, en exploitant les ressources de l’ordinateur victime. |
| **Cheval de troie** | type de malware (Trojen) qui a une apparence légitime mais cache des fonctionnalités malveillantes. |
| **Phishing** | technique frauduleuse qui sert à obtenir des informations sensible (username, password, credit card, social security numbes, …) en se déguisent comme un tiers de confiance (banque, sites de gouvernements, …). |
| **Spamming** | l’utilisation des systèmes de messagerie électronique (e-mail, social media,…) pour l’envoi massive des messages non sollicité pour des raisons de publicité ou des raisons interdit |
| **Ransomware** | malware qui restreint l'accès de l’ordinateur ou données des personnes victimes (chiffrement de tout donnée) et il exige les victimes de payer une rançon (argent en bitcoin) afin d’accéder aux leurs données. |
| **Bombe logique** | block de code insérer dont un système informatique qui déclenchera une fonction malveillante a un moment (temps) / condition déterminé. |
| **Ethical Hacking** | est s'introduit légalement dans des ordinateurs et des appareils pour tester la sécurité d'une organisation, aussi appelé « penetration testing » |

## la Différence entre attaque active et attaque passive :

Les attaques actives sont le type d'attaques dans lesquelles, L'attaquant s'efforce de changer ou de modifier le contenu des messages. L'attaque active est un danger pour l'intégrité et la disponibilité. En raison de l'attaque active, le système est toujours endommagé et les ressources du système peuvent être modifiées. Le plus important est que, lors d'une attaque active, la victime soit informée de l'attaque. Mais les attaques passives sont des d'attaques ou l'attaquant observe le contenu des messages ou copie le contenu des messages. L’attaque passive est un danger pour la confidentialité. En raison d'une attaque passive, il n'y a aucun dommage au système. Le plus important est que dans l'attaque passive, la victime ne soit pas informée de l'attaque.

## La Différence entre Vers et Virus :

La principale différence entre un virus et un ver est que les virus doivent être déclenchés par l'activation de leur hôte, tandis que les vers sont des programmes malveillants autonomes qui peuvent s'auto-répliquer et se propager indépendamment dès qu'ils ont violé le système.

## Type des virus selon les hôte :

|  |  |
| --- | --- |
| **Type** | **Description** |
| **Macro Virus** | Virus qui utilise des scripts de programmation inclue dans les logiciels d’édition de document (MS Word, MS Exel,) |
| **Boot Virus / System Virus** | Type de virus qui attaque les secteurs de boot dans un disque dur ou clé USB |
| **File (binary) Virus** | Ce virus cible les fichiers .EXE ou .COM et les modifient |
| **Email Virus** | Virus utilisent le system email pour se reproduire |

Exercice 4

L’ingénierie sociale est la manipulation psychologique des personnes pour qu'elles accomplissent des actions ou révéler des informations confidentielles. C’est un type d’escroquerie de confiance à des fins de collecte d'informations, de fraude ou d'accès au système (système d’information).

En Juillet 2020, Twitter a été victime d'une attaque d'ingénierie sociale au cours de laquelle des pirates informatiques ont convaincu les employés de Twitter de les aider à détourner des comptes en utilisant leurs outils d'administration d'utilisateurs internes. Ils ont eu accès à des comptes célèbres comme de Joe Biden, Elon Musk, Bill Gates pour convaincre les gens de soutenir leurs communautés en payant des bitcoins.

Source :

* <https://www.vice.com/en/article/jgxd3d/twitter-insider-access-panel-account-hacks-biden-uber-bezos>
* <https://www.youtube.com/watch?v=GcwMUOKGZxc>

|  |
| --- |
| **Mot de passe / username** |
| * Bechar8080 * Bechari80 / Becharia80 * 801212 * 1980BECHAR * B801212 * 121280 * BE08121280 * 1980 |