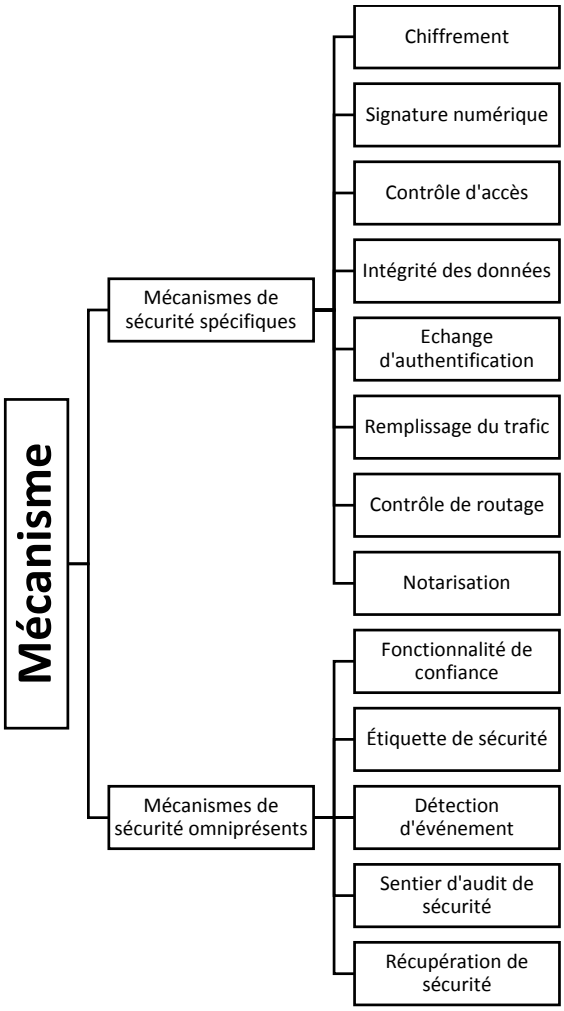
Corrigé TD 1 – Initiation à la Sécurité Informatique

Exercice 1 :

1. Les différents types de sécurité étudiés au cours, ci-arprès:
    - Sécurité Informatique
    - Sécurité du Cloud computing
    - Sécurité des mobiles
    - Sécurité des réseaux
    - Sécurité d'Internet
    - Sécurité du Web
    - …etc

2. Les exigences fondamentales en sécurité informatique sont :
    - **Disponibilité :** Demande que l'information sur le système soit disponible aux personnes autorisées.
    - **Confidentialité :** Demande que l'information sur le système ne puisse être lue que par les personnes autorisées.
    - **Intégrité :** Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.
    - **Non répudiation:** Permettant de garantir qu'une transaction ne peut être niée.
    - **Authentification:** Consistant à assurer que seules les personnes autorisées aient accès aux ressources.
3. Les mécanismes de sécurité définis dans X.800 sont présentés dans la figure suivante.

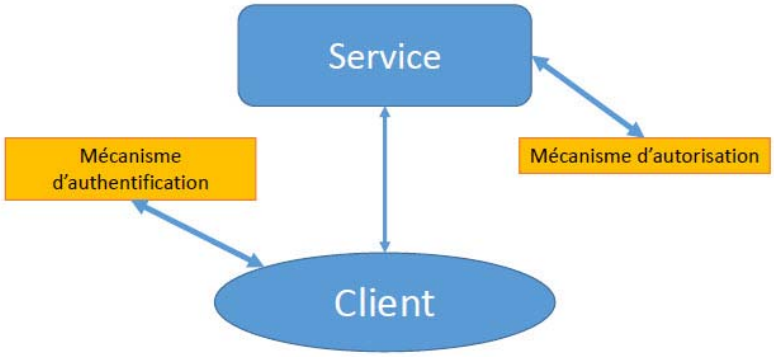


4. La protection de la vie privée (Privacy) est souvent définie comme la capacité de protéger des informations sensibles sur des informations personnellement identifiables, alors que la protection est en réalité un élément de sécurité. D'autres le définissent comme le droit d'être laissé seul. Pourtant, cela ne couvre pas la vie privée d'aujourd'hui dans un monde centré sur les données, d'où la confusion. Dans l'industrie, la vie privée se concentre vraiment sur les concepts suivants:
    - Quelles données devraient être collectées?
    - Quelles sont les utilisations permises?
    - Avec qui pourrait-il être partagé?
    - Combien de temps les données doivent-elles être conservées?
    - Quel est le modèle de contrôle d'accès granulaire approprié?

5. Le contrôle d’accès offre 3 services essentiels:
    - Authentification (qui peut se connecter)
    - Autorisation (ce que les utilisateurs autorisés peuvent faire)
    - Responsabilisation (identifie ce qu'un utilisateur a fait)

Exercice 2 :

1. L'utilisateur doit présenter les informations suivantes :
   - Ce que vous savez (Mots de passe, PIN (Personal Identification Number))
   - Ce que vous avez (Jeton, cartes à puce, codes de passage, RFID)
   - Qui êtes-vous (biométrie comme les empreintes digitales et l'iris scan, signature ou Voix)
2. La différence est dans le nombre de facteurs utilisés.
3. Présentez le schéma "*Authentification vs. Autorisation*" vu au cours.



4. Il y'a deux types d'intégrité de données
   - Intégrité des données : La propriété que les données n'ont pas été modifiée d'une manière non autorisée
   - Intégrité du système: La qualité d'un système lorsqu'il exécute sa fonction prévue de manière intacte, sans manipulation non autorisée
5.

	Libération du contenu du message	Analyse du trafic	Mascarade	Rejouer	Modification des messages	Déni de service
Authentification			Y			
Authentification d'origine des données			Y			
Contrôle d'accès			Y			
Confidentialité	Y					
Confidentialité des flux de trafic		Y				
Intégrité des données				Y	Y	
Non répudiation			Y			
Disponibilité						Y

6.

	Libération du contenu du message	Analyse du trafic	Mascarade	Rejouer	Modification des messages	Déni de service
Chiffrement	Y					
Signature digitale			Y	Y	Y	
Contrôle d'accès	Y	Y	Y	Y		Y
Intégrité des données				Y	Y	
Authentification mutuelle	Y		Y	Y		Y
Remplissage du trafic		Y				
Contrôle de routage	Y	Y				Y
Notarisation			Y	Y	Y	

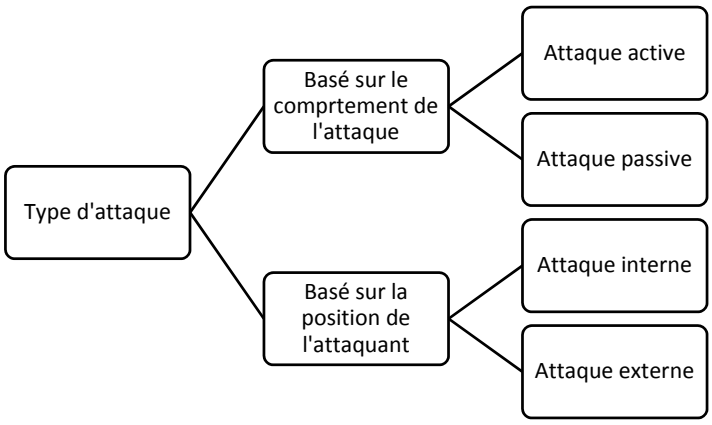
Corrigé TD 2 – Les attaques Informatique

Exercice 1 :

1.

Compétence	Objectif
• **Script Kiddy** - 90% playstation 9% clickomane 1% intelligence - utilise ce que font les autres • **Amateur** - Failles connues - Failles web • **Professionnel** - En equipe - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires) - 0days possibles	• **L'argent** - piratage volumétrique - cryptolocker "killer application" • **Hacktiviste** - "Terroriste" - Anonymous • **Espions** - Etatique - Industriel • **"Petit con"**

2.



Classification des attaques

3.

- L'attaque browser
- L'attaque brute force
- L'attaque DoS
- L'attaque SSL

4. Kaspersky détecte les attaques en temps réel grâce aux applications suivantes :
   - **OAS - On-Access Scan (Analyse à l'accès) :** OAS affiche un flux de détection de logiciels malveillants lors de l'analyse à l'accès, c'est-à-dire lorsque des objets

sont utilisés lors d'opérations d'ouverture, de copie, d'exécution ou de sauvegarde.

- **ODS - On-Demand Scan (Analyse à la demande) :** ODS affiche le flux de détection de logiciels malveillants lors de l'analyse à la demande, lorsque l'utilisateur sélectionne manuellement l'option 'Rechercher des virus' dans le menu contextuel.
- **MAV - Mail Anti Virus :** MAV affiche le flux de détection des logiciels malveillants lors de l'analyse de Mail Anti-Virus lorsque de nouveaux objets apparaissent dans une application de messagerie (Outlook, The Bat, Thunderbird). Le MAV analyse les messages entrants et appelle OAS lors de l'enregistrement des pièces jointes sur un disque.
- **WAV - Web Anti-Virus :** WAVaffiche le flux de détection des logiciels malveillants lors de l'analyse de l'antivirus Web lorsque la page html d'un site Web s'ouvre ou qu'un fichier est téléchargé. Il vérifie les ports spécifiés dans les paramètres Web Anti-Virus.
- **IDS - Intrusion Detection System (Scan de détection d'intrusion) :** IDS affiche le flux de détection des attaques réseau.
- **VUL - Vulnerability Scan:** montre le flux de détection de vulnérabilité.
- **KAS - Kaspersky Anti-Spam :** KAS affiche le trafic de courrier électronique suspect et indésirable découvert par la technologie de filtrage de réputation de Kaspersky Lab.
- **BAD - Botnet Activity Detection (Détection d'activité de botnet):** BAD montre des statistiques sur les adresses IP identifiées des victimes d'attaques DDoS et des serveurs C&C de botnet. Ces statistiques ont été acquises à l'aide du système DDoS Intelligence (partie de la Corrigé Kaspersky DDoS Protection).

5. Pour lancer une attaque physique, on peut faire :
    - Coupure de l'électricité
    - Extinction manuelle de l'ordinateur
    - Ouverture du boîtier de l'ordinateur et vol de disque dur
    - Ecoute du trafic sur le réseau
6. Pour lancer une attaque en réseau, on peut appliquer :
    - Des attaques contre le contrôle d'accès, comme War Driving
    - Des attaques contre la confidentialité, comme Eavesdropping (Ecoute)
    - Des attaques contre l'intégrité, comme 802.11 Data Replay
    - Des attaques contre l'authentification, comme VPN Login Cracking
    - Des attaques contre la disponibilité, comme AP Theft

7. Pour lancer une attaque DoS en réseau, on peut utiliser :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;

- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier ;
- également le fait d'envoyer des milliards d'octets à une box internet.

Exercice 2 :

1. **Les attaques passives** ont trait à l'écoute ou à la surveillance des transmissions. Le courrier électronique, les transferts de fichiers et les échanges client / serveur sont des exemples de transmissions qui peuvent être surveillées.
   Les attaques actives incluent la modification des données transmises et les tentatives d'accès non autorisé aux systèmes informatiques.
2. **Attaques passives :** publication du contenu du message et analyse du trafic.
   Attaques actives : masquerade, relecture, modification des messages et déni de service.
3. **Les attaques de porte d'entrée** exigent les actions d'un utilisateur légitime - par exemple, un logiciel malveillant qui est exécuté lorsqu'un utilisateur légitime ouvre une pièce jointe infectée ou exécute un programme malveillant que l'utilisateur a téléchargé sur Internet.
   Les attaques de porte arrière ne nécessitent pas les actions d'un utilisateur légitime. Au lieu de cela, ils ciblent les vulnérabilités du logiciel serveur qui exécute un ordinateur. Les défauts dans le logiciel serveur peuvent provoquer un programme serveur pour répondre à une demande inattendue de telle manière qu'il donne accès à l'ordinateur. Une attaque de débordement de tampon (buffer overflow attack) est un exemple d'attaque de porte arrière.
4. **Malwares** varient considérablement dans les actions qu'ils prennent une fois que cela compromet l'ordinateur d'une victime. Il peut faire n'importe quoi en annonçant sa présence en affichant un message sur l'écran pour que les sons de l'ordinateur jouent. Il peut également corrompre le système ou tenter d'attaquer d'autres machines en envoyant des courriels infectés, par exemple.
5. **Les pirates blancs** (white-hat hackers) tentent de rendre les systèmes informatiques plus sécurisés en recherchant et signalant des vulnérabilités afin de pouvoir les réparer. Ils peuvent également aider à caractériser de nouveaux virus et à développer des patchs pour eux.
6. **Le 16 mars 2020,**

Emotet.B
Trojan.Heriplor
Trojan.Karagany.B
Trojan.Karagany.B!gm
Trojan.Ismagent