* " " la disponibilité, comme APTheft.

7- pour lancer une attaque DOS en réseau, on peut utiliser :
* l'inondation d'un réseau afin d'empêcher sont fonctionnement
* la perturbation des connexion entre 2 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'octet 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 transfert de fichiers et les échanges client/serveur sont des exemples de transmissions qui peuvent être surveillées.
- Les attaques actives : incluent la modification des données transmise et les tentatives d'accès non autorisé aux système info.

2 - Attaques passives : publication du contenu du msg et analyse du trafic.
- Attaques actives : marquerade, relecture, modification des msg et déni de service.

3 - Les attaques de porte d'entrée: exigent les actions d'un utilisateur légitime. par exp; un logiciel malveillant qui est exécuté lorsqu'un utilisateur légitime ouvre une pièce jointe infectée ou exécute un prgrm malveillant que l'utilisateur à téléchargé sur internet.

- Les attaques du porte arrière: ne necessite 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 prgrm 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 de l'ordinateur jouent. il peut également corrompre le système ou tente d'attaquer d'autres machines en envoyant des receuils infectés.

5- Les pirates Blancs: (white hat hackers) tentent de rendre les systèmes informatiques plus sécurisés en recherchant et signant 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 2018.

Emotet.B
Trojan.Heriplor
Trojan.Karagany.B
Trojan.Karagany.Bzgm.
Trojan.Ismgent.

Série TD n°3 :

exercice 1 :

1- un exploit 0 day est une cyberattaque qui survient le jour même ou une faiblesse est découverte dans un logiciel. À ce stade, il est exploité avant qu'une solution devienne disponible auprès de son créateur.

2- un virus est un fragment de code qui se propage à l'aide d'autres programmes, alors qu'un ver est un programme autonome.

3- L'efficacité de programmes malveillants repose essentiellement à notre équipe sur leur capacité à se propager rapidement en utilisant l'infrastructure des communications.

4- même s'ils ne provoquent aucun dommage sur les machines, les vers utilisent les ressources du réseau pour se propager en déterminant des communications « utiles ».

5- lors du démarrage d'un ordinateur, c'est généralement le SE installé sur le disque dur qui est utilisé par défaut. Le secteur d'amorçage ou certaines parties du SE pour éviter que le code malveillant puisse être détecté.