

Questionnaire :

1) -Un pirate est une personne qui va chercher à piller un système d'information (SI) en détruisant ses protections.

- Un hacker est un passionné qui est spécialiste de la sécurité informatique. Son but est de diffuser l'information. Mais aussi le hacker veut que le savoir et l'information soient ainsi libres et gratuits. Ainsi il se regroupe en communauté pour partager leur compétence.

- La sécurité informatique : Moyens et techniques pour assurer l'intégrité et empêcher la diffusion involontaire des données qui transite dans le système d'informations.

- Le système d'information : Données et ressources(matérielles, logicielles et humaines) qui stock et fait circuler des informations qu'ils contiennent. Plusieurs acteurs interviennent comme les échangent des données, les données y accèdent et ainsi les données sont utilisées.

2) La sécurité informatique est primordiale de nos jours car plusieurs entreprises, qu'elle soit grande ou des PME, seront victimes de cyberattaques. Plus l'entreprise est grande, plus le système d'information sera renforcé par une sécurité informatique importante, comparé par une PME qui elle aura moins de protection donc plus sensible au menace de virus qui peuvent engendrer des pertes financière non négligeable. Les sécurités les plus importante sont d'utiliser un USB sur mesure, surveiller un réseau, la transparence et sensibiliser les employés.

3) L'élément qui attirent les hackers sont les données à caractère sensible (soit les données des utilisateurs) comme les mots de passe, code bancaires, adresses,... et les sites sont parfois inaccessible et qui pose problème dans un système économique est que le fait d'être hacker engendre des pertes financier non négligeable en mettant des virus qui représentent une menace. Cela permet de faire tout savoir, et informé fait que l'entreprise peut être en faillite car elle dévoile des informations que l'entreprise ne doit pas divulguer pour les autres concurrents.

4) Les échelons sur lesquels repose la sécurité informatique sont d'après la pyramide Maslow (du bas en haut de la pyramide) sont en 1er le niveau physique (accès à l'infrastructure), en 2ème au niveau réseau (infrastructure), en 3ème niveau systèmes d'informations (droits d'accès, authentification, contrôle), en 4ème au niveau humain utilisateur (les acteurs doivent comprendre l'importance de leur position) et le 5ème niveau est au niveau de l'organisation (culture de l'entreprise) . Tous ces niveaux correspondent à la sécurité informatique.

5) Les acteurs concernés par le hacking sont

- les entreprises (les dirigeants, les employés) par exemple Plus de 65 % des entreprises visées par la fraude par email se sont vues usurper l'identité de plus de cinq employés,
- les particuliers (par exemple 60% des attaques extrêmement ciblées concernent les utilisateurs individuels et les dirigeant aux échelons inférieurs)
- les écoles : par exemple 301 attaques contre les écoles se sont produites en 2019 contre 124 en 2018. Soit une augmentation de près de 142%. L'école est devenue une nouvelle cible de cyberattaque.
- L'Etat (un pays ou une nation) : par exemple pendant les élections américaine 2020, l'Etat américain offre une récompense à celui qui démasque toute personne qui apporterait des informations sur une possible ingérence étrangère

6) Le profil général du hacker est qu'il accède illégalement les données personnels de personnes (client, employeur...) même des grandes entreprises. C'est un personnage très cultivé, qui est très technique et avec beaucoup d'expérience. Il connaît l'histoire de leur statut, des grands acteurs du mouvement. Celui-ci se tient informé de tout ce qui appartient à son domaine et il utilise son savoir pour découvrir les choses auxquelles il ne devrait pas savoir.

7) L'éthique du hacker définit par Steven levy en 1984 sont que toute information est par nature libre et gratuite. Que l'accès aux ordinateurs devrait être total, illimité, possible pour tout le monde, que la décentralisation des données doit être encouragée. Les hackers devraient être jugés sur le hacking et non sur les hiérarchies sociales telles que le diplôme, l'âge ou le grade. Il y a aussi qu'on peut créer de l'art et de la beauté avec un ordinateur et que les ordinateurs peuvent améliorer la vie.

8) La transformation de Kevin Mitnick vis-à-vis de la société est que celui-ci est un ancien pirate surnommé "Le Condor". Il accède illégalement aux bases de données des clients d'une entreprise puis à des systèmes de d'autres entreprises comme Nokia. Il fait donc son premier délit en 1980. Puis il a eu une première condamnation en 1983 car il a tenté une intrusion dans le réseau du Pentagone. Aussi en 1987 il est de nouveau arrêté par la police pour utilisation illégale de numéros de cartes de paiement téléphoniques. Arrêté par le FBI une première fois, puis ensuite en 1989 il passe 8 mois en prison, il devient un fugitif pour être retrouvé 2 ans après. Il a eu un procès et doit 1,5 millions de dollars en dédommagement. Depuis 2000 il fait du conseil de sécurité (consultant) pour des entreprises du Fortune 500.

9) Les 5 grands principes à mettre en oeuvre contre une cyberattaque sont:

- L'intégrité des données (garder les forme inutiles et donc pas d'altération)
- La confidentialité (seules les personnes habilités ont accès au données)
- La disponibilité (avoir accès à n'importe quel moment (au système, services et ressources)
- La non-répudiation des données (une transaction ne peut être niée par aucun des correspondants)
- L'authentification (assurer de l'identité d'un utilisateur avant l'échange de données)

10) Les différents types de hackers pour la finalité sont :

Pour le Black hats : de pénétrer par effraction dans les systèmes, pour leur satisfaction personnelle, voire financière.

Pour les Crackers : Il y a la finalité de nuire (cyberterrorisme).

Pour les Grey hats : leur finalité n'est pas forcément mauvaise, peut commettre occasionnellement un délit. Il n'endommage pas le système pénétré en prévenant le propriétaire et prévient leur communauté.

Pour les white hats : Il aide à la sécurisation du système, sans tirer de bénéfice de manière illicite, il prône la divulgation totale de leur découverte et met au courant les auteurs des vulnérabilités qui les touchent.

Pour les pentesters : il y a un suivi des méthodologies référencées et utilise des outils de reporting pour répertorier les incidents détectés.

Pour les Scripts Kiddies : Il y a la vantardise, le fait de récupérer les exploits laissés par les white hats sur les outils publics et exécuté sur des machines provoquant des pannes volontaires.

Pour les hacker universitaires : Enfin, il partage sa connaissance avec autrui, travaillant en communauté et sont à l'origine d' internet et du système d'exploitation Unix.

Les différents type de hacker pour leur profil sont :

Pour les Black hats : révoltés contre le système, frôlent le limites de la loi, on une éthique, très cultivés et appréciés par l'entreprises pour leur compétences et expert technique avec beaucoup d'expérience

Pour les Cracker : déplombeur de logiciels (appartiennent au black hats), sont dangereux, sont à l'origine des virus, chevaux de Troie et logiciels espions.

Pour le Grey hats : ce sont des experts techniques avec beaucoup d'expérience, très cultivés, sont joueurs, curieux et même esprit d'un white hat avec une philosophie de divulgation différente.

Pour les white hats : ce sont des experts techniques avec beaucoup d'expérience, très cultivés, bidouilleur des système d'information et recherche par les entreprises

Pour les pentesters : il fait de sa passion un métier, il en vit, à une éthique ,des experts techniques avec beaucoup d'expérience et très cultivé.

Pour les Scripts Kiddies: c'est un adolescents sans expérience et sans connaissance, réutilisent des codes ou des programmes prêts à l'emploi, sont dangereux et n'a aucune notion d'éthique du hacker.

Pour les hackers universitaires: ils sont libres associés au mouvement open source (logiciel libre), pour eux l'information est libre n'appartient à personne, cultivé, on veut échanger et expert en réseau et en technologie avec beaucoup d'expérience.