Travaux Dirigés [série n°2] - Les attaques Informatiques

Questions :

1. Qu'est-ce qu'un malware ?
2. Quels sont les types de malwares les plus courants ?
3. Comment les malwares se propagent-ils ?
4. Comment puis-je éviter de télécharger un malware ?
5. Que dois-je faire si je pense que mon ordinateur est infecté par un malware ?
6. Comment un malware peut-il endommager mon système informatique ?
7. Comment puis-je éviter de propager un malware à d'autres ordinateurs ?
8. Quelles sont les différences entre les malwares les plus courants ?
9. Quelle(s) technique(s) utilise un antivirus pour détecter les programmes malveillants ?
- 10.** Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
11. Quelle est la différence entre les menaces de sécurité passives et actives ?
12. Quelle est la différence entre une attaque de porte d'entrée et une attaque de porte arrière (front-door attack and a back-door attack). Donnez un exemple de chacun ?
13. Comment les pirates informatiques opèrent ?
14. Décrivez les façons dont les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sûrs ?
15. Qu'est-ce qu'une porte dérobée (backdoor) ?
16. Décrire les étapes d'une attaque ?
17. Quels sont les techniques d'attaques réseaux ?
18. Il arrive régulièrement que des codes malveillants réussissent à persister sur une machine sans être détectés par les antivirus installés par la victime de l'infection. Décrire deux techniques différentes qui permettent à un code malveillant de ne pas être détecté par les logiciels antivirus.
19. En général, les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus. Pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
20. Quels sont les différents types d'IDS