Aide à la révision

Généralités

1. Qu'est ce qu'un système d'information ?
2. Quels sont les composants d'un risque ?
3. Quelles sont les deux définitions du risque ?
4. Quels sont les trois types d'impacts pris en considération en sécurité des systèmes d'information ? Expliquez chacun d'eux.
5. Quelle est la principale vulnérabilité en sécurité des SI ?
6. Qu'est ce que l'ingénierie sociale ?
7. A quoi correspondent les attaques par dictionnaire et les attaques par brute force ?
8. Qu'est ce qu'une "zero day attack" ?
9. Qu'est qu'une DMZ ? Quelle est son utilité ?
10. Qu'est ce qu'un serveur mandataire ? Quelle est son utilité ?
11. Qu'est ce qu'un IDS ? Quelle est son utilité ?
12. Qu'est ce qu'un "pot de miel" ? Quelle est son utilité ?
13. Que sont les CERT ? Quel est leur rôle ?
14. Qu'est ce que la CNIL ? Quel est son rôle ?
15. Qu'est ce que l'ISO ? Quel est son apport dans le domaine de la sécurité des SI ?
16. Qu'est ce qu'une politique de sécurité des SI ?
17. Quelle est la nouvelle approche de la sécurité (qui date d'il y a une dizaine d'année) ?

Chiffrement

18. Que permettent de garantir les techniques de chiffrement ? Autrement dit, quels sont les champs d'application du chiffrement ?
19. Qu'est ce que le chiffrement symétrique ?
20. Qu'est ce que le chiffrement asymétrique ?
21. Qu'est ce qu'une clé de session ?
22. A quoi correspond un certificat électronique ?
23. Qu'est ce qu'une PKI ? Quel est son rôle ?
24. Quels sont les deux mécanismes sur lesquels reposent les méthodes de chiffrement ? Expliquez chacun d'eux.
25. Quel est le principe sur lequel repose le code de César ?
26. Qu'est ce que la machine Enigma ? Sur quel procédé de chiffrement repose son fonctionnement ?
27. Qu'est ce que le scytale de Sparte ? Sur quel procédé de chiffrement repose son fonctionnement ?
28. Qu'est ce que le cylindre de Jefferson ? Sur quel procédé de chiffrement repose son fonctionnement ?
29. Citez deux algorithmes de chiffrement symétrique ayant été retenus comme standard par le NIST ?
30. Qu'est-ce que le 3DES ?

31. Quelle est la principale difficulté (vulnérabilité) d'utilisation d'une méthode de chiffrement symétrique ?
32. A quoi sert la méthode de Diffie-Hellman ?
33. Qu'est ce que RSA ?
34. Comment chiffre-t-on un message avec RSA ?
35. Comment signe-t-on un message avec RSA ?
36. A quoi sert la fonction de hachage dans le cadre de la signature d'un mail avec RSA ?
37. Alice récupère un certificat correspondant à Bob auprès d'une PKI. Comment procède-t-elle pour vérifier la validité de celui-ci ?
38. A quoi correspond PGP ?
39. Effectuez un comparatif (avantages/inconvénients) des méthodes de chiffrement symétrique par rapport aux méthodes de chiffrement asymétrique.
40. Qu'est ce qu'une méthode de chiffrement hybride ?
41. Comment fonctionne un échange entre un navigateur web d'un client et un serveur web mettant en œuvre HTTPS ?
42. Qu'est ce que le réseau TOR ?
43. Expliquez les principes de chiffrement mis en œuvre par Tor.
44. Le réseau Tor permet-il de garantir l'anonymat de ses utilisateurs ?
45. Le réseau Tor permet-il de garantir la confidentialité des données échangées par son biais ?
46. Quels sont les soucis /limitations présentés par le réseau Tor ?
47. Qu'est ce que le bitcoin ?
48. Qu'est ce que la blockchain ?
49. Expliquez pourquoi une transaction inscrite dans la blockchain est infalsifiable.

Filtrage

50. Quels sont les différents usages que l'on peut faire d'un pare-feu ?
51. Quels sont les deux types de pare-feu utilisés ?
52. A quoi correspond le filtrage "stateful" pour un pare-feu ? Quel est l'intérêt de ce type de procédé pour le traitement du protocole FTP ?
53. Quelles sont les limites d'utilisation d'un pare-feu (cadre dans lequel il n'est pas opérationnel) ?
54. Qu'est ce qu'une matrice des flux ? Quelle est son utilité ?

Sécurité Web

55. Quelles sont les principales vulnérabilités présentes dans le top 10 de l'OWASP ?
56. Qu'est-ce qu'une attaque par injection ?
57. Qu'est ce qu'une attaque en XSS ? Quel objectif vise-t-elle ?
58. Qu'est ce qu'une attaque en CSRF ? Quel objectif vise-t-elle ?
59. Quels sont les principaux mécanismes de sécurité que l'on peut mettre en œuvre de façon à sécuriser un service web et son usage ?

ISO27001

60. Quelles sont les principales normes composant la famille de normes ISO27001 et de quoi traite principalement chacune d'elles ?
61. Qu'est ce qu'un SMSI ?
62. Quelle est l'utilité d'un SMSI ? Quels sont ses avantages ?
63. Qu'est ce que le PDCA ?
64. A quoi correspond la phase Plan du PDCA pour la norme ISO27001?
65. A quoi correspond la phase DO du PDCA pour la norme ISO27001?
66. A quoi correspond la phase CHECK du PDCA pour la norme ISO27001?
67. A quoi correspond la phase ACT du PDCA pour la norme ISO27001?
68. Que traite la norme ISO27002 ?
69. Quelles sont les phases composant une gestion des risques ?
70. Quels sont les différents traitements possibles d'un risque ?
71. Qu'est ce qu'une DdA ? A quoi sert-elle ?

En plus du questionnaire :

- Revoir les exercices sur le chiffrement ;
- Revoir les exercices sur la norme ISO27001 (surtout l'exercice 3) ;

Hors programme de révision (ne pas revoir)

- La partie du cours sur le pare-feu concernant Netfilter et le filtrage sous Linux.
- Les exercices sur le filtrage
- Les différents TPs