Intra A20

1. La disponibilité est une priorité de vivacité (liveness)

Rép : Vrai

2. Complétez la phrase, un risque est la combinaison _____ et d'une menace ?

Rép : d'une vulnérabilité

3. Lorsqu'un acteur malveillant récupère ou vole le SecureID d'authentification d'un employé d'une compagnie qu'il souhaite attaquer, lequel des attributs suivants de l'analyse de risque est affecté :

Rép : Opportunité

4. Dans un cyber café
   Un utilisateur malveillant s'installe dans un cyber café et essaye d'intercepter des mots de passe et numéros de carte de crédit sur le réseau Wi-Fi du café pour réaliser de la fraude bancaire par Internet.

Rép : D'une menace?

5. Dans un cyber café (suite)

   Le cyber-café utilise le protocole WEP pour chiffrer les communications WIFI et il est possible de casser ce protocole en quelques secondes.

Rép : D'une vulnérabilité ?

6. Dans un cyber café (suite)

   Dans un cyber café, vous utilisez toujours un VPN pour établir une connexion chiffrée pour accéder à vos applications.

Rép : D'une contre-mesure ?

7. Quelle est l'erreur dans l'analyse de risque suivante?

Rép : La capacité dans B est trop élevé

8. Chiffrement de Vigenere
   Vous utilisez le chiffrement de Vigenere avec la clé NOEL. Votre amie Alice vous envoie le message chiffré suivant WCCPHLLYZSHRSR. Quel est le message en clair correspondant ?

Rép : JOYEUXHALLOWEEN

9. Chiffrement de Vigenere (Explication de la question précédente)

Rép : Dans le cours de crypto 1, dans l'acétate 50 on peut voir le fonctionnement de l'algorithme de Vigenere. On a une source, le codage, la clé et le chiffrement.

   En appliquant…. Voir pdf

10. Chiffrement de Vigenere (suite)
    Avec le chiffrement de Vigenere, un caractère n'est pas toujours chiffré de la même façon. Le chiffrement de Vigenere est donc résistant à la cryptanalyse par analyse fréquentielle.

Rép : Faux

11. Chiffrement de Vernam
    Pour que le chiffrement de Vernam soit parfaitement sécuritaire, il faut utiliser une clé aléatoire de la même longueur que le message que l'on veut chiffrer.

Rép : Vrai

12. Chiffrement de Vernam
    Le chiffrement de Vernam ne peut être utilisé qu'avec une clé binaire composé de 0 et de 1.

Rép : Faux

13. Chiffrement de Vernam
    Le chiffrement de Vernam peut être considéré comme un cas particulier du chiffrement de Vigenere avec une clé aléatoire égale à la taille du message à chiffrer.

Rép : Vrai

14. La loi de Moore stipule que la puissance de calcul des ordinateurs disponibles sur le marché double à chaque 18 mois. Combien de bits de clés serait-il nécessaire d'ajouter à un algorithme de cryptographie symétrique à 128 bits pour compenser pour l'effet de la Loi de Moore sur une période de 15 ans.

Rép : 10 bits

15. Le chien de Mickey Mouse est très triste ces jours-ci. La « planète » qui jadis portait le nom n'est plus une planète, car elle a été déclassée… Mais en termes de sécurité, à combien de bits de plus équivaut une année sur Pluton, en comparaison à une année sur la Terre? (Note : La Terre tourne autour du soleil 250 fois plus vite que Pluton).

Rép : Environ 8 bits

16. On considère une source qui génère aléatoirement trois chiffres 0,1 et 2. La probabilité d'apparition du 0 est ½ et celle d'apparition du 1 est ¼ et celle du 2 est également ¼. On utilise cette source pour générer une chaine de 10 chiffres. Quelle est l'entropie de cette chaîne :

Rép : 15 bits

17. (Explication de la question précédente)
    On considère une source qui génère aléatoirement trois chiffres 0,1 et 2. La probabilité d'apparition du 0 est ½ et celle d'apparition du 1 est ¼ et celle du 2 est également ¼. On utilise cette source pour générer une chaine de 10 chiffres.

Rép : Voir calcul question 16

18. 20 mille lieues sur les mers
    Une source qui génère des phrases en tirant au hasard des mots dans le roman de Jules Verne « 20 mille lieues sous les mers » est une source markovienne aléatoire :

Rép : Vrai

19. 20 mille lieues sous les mers (suite)
    On considère une source qui génère des « phrases de passe » en tirant au hasard des mots dans le roman de Jules Verne « 20 mille lieues sous les mers ». Cette source est potentiellement vulnérable à une attaque par analyse fréquentielle

Rép : Vrai

20. 20 mille lieues sous les mers (suite)
    Une source qui génère des phrases en tirant au hasard un mot dans la première page du roman de Jules Verne « 20 mille lieues sous la mer », puis un mot dans la deuxième page, un mot dans la troisième page, et ainsi de suite, est une source markovienne aléatoire :

Rép : Vrai (Voir explication pdf)

21. (Explication de la question précédente)
    Une source qui génère des phrases en tirant au hasard un mot dans la première page du roman de Jules Verne « 20 mille lieues sous la mer », puis un mot dans la deuxième page, un mot dans la troisième page, et ainsi de suite, est une source markovienne aléatoire.

Rép : Cette source est une source markovienne aléatoire puisqu'on choisit un mot dans chaque page, et ce mot ne dépend pas du mot choisit dans la page précédente.

22. 20 mille lieues sous les mers (suite)
    On considère un roman qui est écrit avec seulement 4 mots : papa, maman, oui, non (un roman que Jules Vernes a écrit quand il était tout petit)

Rép : La phrase générée par source1 a 10 bits d'entropie de plus que celle générée par source2

23. 20 mille lieues sous les mers (Explication de la question précédente)
    On considère un roman qui est écrit avec seulement 4 mots : papa, maman, oui, non (un roman que Jules Vernes a écrit quand il était tout petit)

24. Vive la brocante
    Vous êtes très contents car vous avez découvert un vieux PC sous Windows 3. Vous l'avez payé un peu cher car le vendeur vous a prétendu qu'il avait appartenu au célèbre hacker Kévin Mitnick. Le vendeur vous a également dit que le PC était protégé par un mot de passe par un mot de passe qu'il ne connaissait pas. Vous avez ainsi pu négocier un rabais.

Rép : Environ 1 jour

25. Vive la brocante (suite)
    Malheureusement, l'attaque par dictionnaire ne donne aucun résultat. Vous envisagez donc une attaque par force brute. Vous supposez que le mot de passe est codé sur 8 caractères alphabétiques (caractères minuscules a-z, majuscules A-Z).

Rép : Environ 1 700 000 ans

26. Vive la brocante (suite)
    Quelle est l'entropie d'un mot de passe codé sur 8 caractères alphabétiques (caractères minuscules a-z, majuscules A-Z) générés aléatoirement ?

Rép : Environ 45,6 bits

27. Vivre la brocante (suite)
    Vous renoncez à mener cette attaque par force brute et vous êtes contrarié d'avoir payé ce PC aussi chez. Cependant, en essayant de taper quelques mots de passe au hasard, vous constatez un comportement étrange. Dans certains cas, lorsque vous tapez le premier caractère du mot de passe, le curseur avance, et dans d'autres cas, il n'avance pas.

Rép : 6 minutes 56 secondes (Voir explication)

28. Vivre la brocante (Explication de la question précédente)
    Vous renoncez à mener cette attaque par force brute et vous êtes contrarié d'avoir payé ce PC aussi chez. Cependant, en essayant de taper quelques mots de passe au hasard, vous constatez un comportement étrange. Dans certains cas, lorsque vous tapez le premier caractère du mot de passe, le curseur avance, et dans d'autres cas, il n'avance pas.

Rép : Voir le pdf

29. Le protocole de chiffrement 3DES utilise :

Rép : 2 clés et 3 chiffrements

30. Nous sommes en 2050 et il n'est plus recommandé d'utiliser le protocole AES avec une clé de 128 bits. Votre directeur vous demande de comparer deux solutions : (1) chiffrer les documents une deuxième fois avec une autre clé de 128 bits, (2) déchiffrer tous les documents et les rechiffrer avec une clé de 256 bits. Vous répondez :

Rép : La solution 2 est préférable

31. Avec le protocole RSA, pour déchiffrer un message envoyé par Alice, Bob doit utiliser :

Rép : Sa propre clé privée

32. Avec le protocole RSA, pour vérifier un message signé par Alice, Bob doit utiliser :

Rép : La clé publique d'Alice

33. Il est recommandé d'utiliser des clés plus longues pour le chiffrement RSA que pour le chiffrement AES. Mais, même à longueur de clés égales, le chiffrement avec RSA serait plus lent qu'avec AES :

    Rép : Vrai

34. Votre mot de passe est une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 4000 mots. D'un point de vue de sécurité, votre mot de passe est équivalent à une clé de chiffrement de longueur :

Rép : Environ 48 bits (Voir explication)

35. (Explication de la question précédente)
    Votre mot de passe est une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 4000 mots. D'un point de vue de sécurité, votre mot de passe est équivalent à une clé de chiffrement de quelle longueur ?

Rép : Voir explication pdf

36. Votre mot de passe est une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 4000 mots.) Si vous deviez choisir un mot de passe composé de caractères alphabétiques (lettres minuscules a-z) et des chiffres 0 et 1, quel devrait être la longueur de ce mot de passe pour une sécurité équivalente ?

Rép : Environ 10 caractères

37. (Explication de la question précédente)
    Votre mot de passe est une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 4000 mots.) Si vous deviez choisir un mot de passe composé de caractères alphabétiques (lettres minuscules a-z) et des chiffres 0 et 1, quel devrait être la longueur de ce mot de passe pour une sécurité équivalente ?

Rép : voir explication pdf

38. Laquelle de ces conditions n'est pas nécessaire pour assurer la sécurité d'un système de signature numérique avec hachage cryptographique ,

Rép : Une entropie élevée de la source qui génère les textes à signer

39. Laquelle de ces affirmations est vraie :

Rép : La technologie par reconnaissance rétinienne est la technologie biométrique la plus difficile à contrefaire

40. La technologie par reconnaissance de l'iris repose sur 266 caractéristiques. La probabilité de similitude est extrêmement faible : 1/ (10 ^78). Cela correspond à la probabilité de trouver du premier coup un mot de passe alphanumérique (composé de caractères minuscules a-z, et de chiffres 0-9) d'une longueur de :

Rép : Environ 50 caractères

41. (Explication de la question précédente)
    La technologie par reconnaissance de l'iris repose sur 266 caractéristiques. La probabilité de similitude est extrêmement faible : 1/ (10 ^78).

Rép : Voir explication pdf

42. Sous Linux, pour définir les droits suivants sur le fichier exam : -rwxr-x—x 1 david profs 7627 Oct 1 12 :50 exam
    David doit exécuter la commande suivante :

Rép : chmod 751 exam

43. Sous Linux, la commande « chmod 754 exam » est équivalente à la commande « chmod u=rwx, g=rx, 0=r exam » sont équivalentes.

Rép : Vrai

44. Dans le système de contrôle d'accès discrétionnaire implanté sous Linux, quelle affirmation est fausse :

Rép : Le groupe associé à un objet ne peut pas avoir plus de droit que le propriétaire de cet objet

45. Dans les distributions Linux modernes, les informations sur les mots de passe des usagers se trouvent dans le fichier /etc/passwd.

Rép : Faux

46. Le modèle de Bell et Lapadula ne protège pas l'intégrité des données

Rép : Vrai

47. Dans le modèle RBAC, la contrainte « dans une même session, il n'est pas possible d'activer les rôles professeur et étudiant », est une contrainte de type :

Rép : Séparation dynamique des pouvoirs (DSOD)

48. Le modèle ABAC repose sur les attributs. On ne peut donc pas utiliser le concept de rôle quand on définit une politique d'autorisation avec le modèle ABAC

Rép : Faux

49. Dans le modèle ABAC, le composant qui accorde ou refuse un accès s'appelle :

Le PEP (Policy Enforcement Point)

50. Quelle affirmation concernant XACML est fausse :

Rép : XACML permet de gérer le SSO (Single Sign On)