1. La clé WEP est utilisée pour chiffrer mais pas pour déchiffrer

   ____ Vrai _____Faux

2. La méthode d'authentification qui utilise WEP s'appelle
   a. Shared key authentication
   b. Wired equivalent privacy authentication
   c. Weak authentication
   d. Open system authentication
3. Même si la méthode ne va pas être utilisée, la norme 802.11 stipule que la méthode d'authentification qui utilise WEP doit obligatoirement être implémentée

   ____ Vrai _____Faux

4. Qu'est-ce que WEP veut dire :
   a. Wireless Equivalent Privacy
   b. Wired Equivalent Privay
   c. Wireless Encryption Protocol
   d. Wired equivalency protocol
5. Dans sa version originale, combien de bits secrets WEP utilise-t-il pour encrypter les données ? (les bits secrets sont ceux qui sont sensés être connus seulement par les ayant droit)
   a. 64
   b. 104
   c. 40
   d. 128
6. Quel est le nombre d'octets ajouté à une trame de données chiffrée avec WEP par rapport à la même trame en clair ?
   a. 4
   b. 8
   c. 7
   d. 0
7. Pour les transmissions en clair, la taille d'une trame ACK de niveau MAC est de 14 Octets. Quel est sa taille lorsque WEP est utilisé ?
   a. 14
   b. 24
   c. 23
   d. 18

8. Le vecteur d'initialisation dans WEP
   _____ A la même longueur qu'une adresse MAC (48 bits)

   _____ Est transmis en claire

   _____ Est le même pour toutes les trames

9. Vous avez accès à un réseau comme celui de la figure, dans lequel une station est associée à un AP et celui-ci est connecté à un HUB. Le HUB est connecté à un routeur (pas montré dans la figure). La sécurité WEP 64 bits est utiliseée. Vous pouvez enregistrer les trames 802.11 et, puisque l'on vous donne accès au HUB, vous avez également accès aux trames Ethernet. Vous concaténez une suite de 24 bits fixes avec chacune des combinaisons possibles de 40 bits et vous utilisez chacune de ces séquences de 64 bits comme semence pour produire des suites RC4. Vous commencez alors à capturer des trames aussi bien dans le réseau WiFi que dans le réseau Ethernet. Combien de trames devez-vous capturer en moyenne avant de pouvoir trouver la clé WEP ? Marquez d'une croix votre réponse.

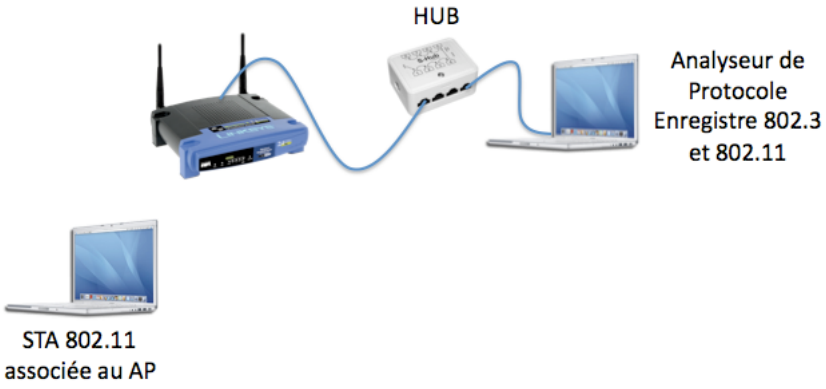
1 trame _____

2^{40} trames _____

2^{23} trames _____

2^{24} trames _____

2^{64} trames _____



10. Lesquelles des affirmations suivantes sont vraies pour WEP ?

_____ L'authentification entre le client et l'AP est mutuelle (tant le client que l'AP s'authentifie auprès de l'autre)

_____ La confidentialité est assurée par le vecteur d'initialisation IV

_____ Il est possible de hacker le WEP si l'on enregistre un nombre suffisamment élevé de vecteurs d'initialisation faibles

_____ La longueur de la clé ne résolue pas les faiblesses principales de WEP

11. Lorsque WEP est utilisé, la confidentialité des données transmises est assurée par le vecteur d'initialisation.

Vrai_____ Faux_____

12. Lorsque WEP est utilisé pour l'authentification, celle-ci est mutuelle.

Vrai_____ Faux_____

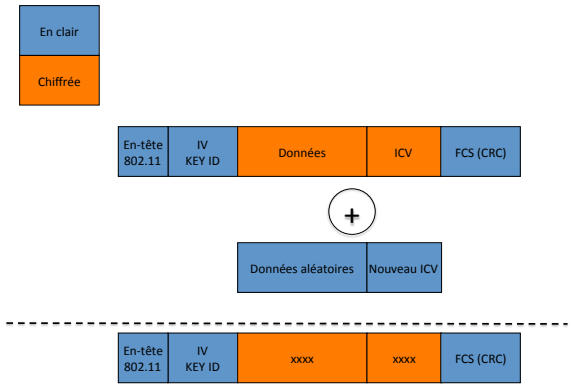
13. Vous capturez une trame de données chiffrée avec une clé WEP que vous ne connaissez pas. Vous utilisez un outil qui pour changer quelques bits au hasard dans la partie données de la trame et vous transmettez la trame modifiée. Vous constatez alors que la trame n'a pas été acceptée par la Station destinatrice. Quelle partie de la trame, la station a-t-elle utilisé pour déterminer que la trame a été trafiquée ?

Réponse :

14. Vous capturez une trame de données chiffrée avec une clé WEP que vous ne connaissez pas. Vous constatez que la longueur du PDU LLC transporté par la trame est de 100 octets. Vous prenez 100 octets aléatoires, vous calculez le l'ICV pour ces données et vous remplacez l'ICV de la trame avec celui que vous venez de calculez. Si vous transmettez cette nouvelle trame, sera-t-elle rejetée par la station destinatrice ?

Oui_____ Non_____

15. Vous capturez une trame de données chiffrée avec une clé WEP que vous ne connaissez pas. Analysant la trame, vous constatez que la longueur du PDU LLC transporté par la trame est de 100 octets. Le processus décrit en ce qui suit est illustré à la figure : Vous prenez 100 octets aléatoires que nous appellerons « A », vous calculez le l'ICV qui correspondrait à « A », vous concaténez « A » et son ICV et vous additionnez le résultat modulo-2 au PDU || ICV chiffrés qui apparaissaient originalement dans la trame. Si vous transmettez cette nouvelle trame, sera-t-elle rejetée par la station destinatrice ?


En clair
Chiffrée
En-tête 802.11
IV KEY ID
Données
ICV
FCS (CRC)
+
Données aléatoires
Nouveau ICV
En-tête 802.11
IV KEY ID
xxxx
xxxx
FCS (CRC)

Oui_____ Non_____