

1. Avec quel message ou trame le serveur d'authentification s'authentifie-t-il auprès du suppliant dans WPA personnel?

Réponse : _____

2. Avec quel message ou trame le serveur d'authentification s'authentifie-t-il auprès du suppliant dans WEP?

Réponse : _____

3. Pour utiliser WPA, les stations doivent avoir une adresse IP dans le même sous réseau que le serveur d'authentification

_____ Vrai X Faux

4. A quoi le 4-way handshake sert-il dans WPA?

_____ Authentification

_____ Intégrité

_____ Confidentialité

5. Lequel ou lesquels de ces protocoles ou algorithmes est/sont utilisé-s dans WPA PSK

_____ PEAP

_____ AES

_____ RC4

6. Laquelle ou lesquelles des affirmations suivantes sont vraies pour CCMP ?

_____ L'intégrité des trames est assurée par le MIC

_____ CCMP ne peut pas être utilisé sans serveur d'authentification

_____ Est fondamental pour l'authentification lors du 4-way handshake

_____ L'algorithme de chiffrement utilisé est le AES

7. Dans un réseau WPA-PSK, un hacker s'empare de la KEK (mais pas des autres clés). Il l'utilise pour chiffrer une nouvelle clé qu'il envoie à une STA en se faisant passer pour l'AP afin de la faire croire que la GTK a été changée. La STA en question, tombe-t-elle dans le piège ?

_____ Vraie

_____ Faux

Pourquoi ?
