Quizz

1) Qu'est-ce qu'une faille Evil Twin ?

- ☐ Une réplique d'un appareil Bluetooth pour une connexion à des fins malveillantes.
- ☐ Une réplique d'un point d'accès Wifi pour tromper les utilisateurs.
- ☐ Une réplique d'une adresse IP pour se connecter comme un autre ordinateur.
- ☐ L'utilisation d'un VPN pour se connecter à des fins malveillantes.

2) Où peuvent avoir lieu les attaques EvilTwin ?

- ☐ Dans un café.
- ☐ Dans un lieu public.
- ☐ Le plus souvent chez soi.
- ☐ Les trois propositions précédentes sont vraies.

3) Donnez une utilisation malveillante pouvant être réalisé à partir de cette faille :

- ☐ Contrôler l'appareil sur lequel on est connecté à distance.
- ☐ Récupérer des informations personnelles par exemple bancaire.
- ☐ Entendre les appels téléphoniques de l'utilisateur connecté.
- ☐ Détruire l'appareil connecté.

4) Quels sont les moyens de se protéger contre les attaques d'un Evil Twin ?

- ☐ Utiliser par exemple un VPN ou un WIPS.
- ☐ Vérifier avec la personne que l'appareil Bluetooth correspond bien.
- ☐ Utiliser un WIPS et un réseau 5G.
- ☐ Aucune des réponses ci-dessus.

5) Que signifie l'acronyme WIPS ?

- ☐ Wireless Intrusion Preparation System .
- ☐ Wireless Intrusion Prevention Software .
- ☐ Wireless Intrusion Prevention System .
- ☐ Wireless Integration Prevention System.

6) Que fait un WIPS ?

- ☐ Il permet l'écoute radio et la reconnaissance de modèle d'attaque.
- ☐ Il créer un point d'accès WiFi sécurisé.
- ☐ Il permet de repérer les appareils Bluetooth de confiance.
- ☐ Il récupère les informations relatives à une connexion permanente.

7) Quels sont les composant d'un WIPS ?

- ☐ Un système radio, un serveur de management, une connexion IPV4.
- ☐ Un système radio, un serveur de management, une console de management.
- ☐ Un système Bluetooth, un serveur de management, une console de management.
- ☐ Un système radio, un serveur DNS, une console de management.