6 Menaces visant le réseau WLAN

Vidéo – Menaces WLAN

Cette vidéo présentera les points suivants :

- Interception de données
- Intrus sans fil
- Attaques par déni de service (DoS)
- Points d'accès escrocs

Présentation de la sécurité sans fil

Un WLAN est ouvert à toute personne à portée d'un point d'accès et aux informations d'identification appropriées à lui associer.

Les attaques peuvent être générées par des étrangers, des employés mécontents et même involontairement par des employés. Les réseaux sans fil sont particulièrement sensibles à plusieurs menaces, notamment:

- Interception de données
- Intrus sans fil
- Attaques par déni de service (DoS)
- Points d'accès escrocs

les Attaques DoS

Les attaques DoS sans fil peuvent être le résultat de ce qui suit:

- Périphériques mal configurés
- Un utilisateur malveillant interférant intentionnellement avec la communication sans fil
- Interférence accidentelle

Pour minimiser le risque d'une attaque DoS en raison d'appareils mal configurés et d'attaques malveillantes, renforcez tous les appareils, sécurisez les mots de passe, créez des sauvegardes et assurez-vous que toutes les modifications de configuration sont intégrées en dehors des heures d'ouverture.

Les Points d'Accès Non Autorisés

- Un point d'accès non autorisé est un point d'accès ou un routeur sans fil qui a été connecté à un réseau d'entreprise sans autorisation explicite et conformément à la politique de l'entreprise.
- Une fois connecté, l'escroc AP peut être utilisé par un attaquant pour capturer des adresses MAC, capturer des paquets de données, accéder à des ressources réseau ou lancer une attaque de type homme-au-milieu.
- Un point d'accès au réseau personnel pourrait également être utilisé comme point d'accès non autorisé. Par exemple, un utilisateur avec un accès réseau sécurisé permet à son hôte Windows autorisé de devenir un point d'accès Wi-Fi.
- Pour empêcher l'installation de points d'accès non autorisés, les organisations doivent configurer les WLC avec des stratégies de points d'accès malveillants et utiliser un logiciel de surveillance pour surveiller activement le spectre radioélectrique des points d'accès non autorisés.

Attaque d'Homme-au-Milieu

Dans une attaque d'homme-au-milieu (MITM), le pirate est positionné entre deux entités légitimes afin de lire ou de modifier les données qui transitent entre les deux parties. Une attaque «evil twin AP» est une attaque MITM sans fil populaire où un attaquant introduit un AP escroc et le configure avec le même SSID qu'un AP légitime

Le processus commence par l'identification des périphériques légitimes sur le WLAN. Pour ce faire, les utilisateurs doivent être authentifiés. Une fois que tous les périphériques légitimes sont connus, le réseau peut être surveillé pour détecter les périphériques ou le trafic anormaux.