Faille Evil Twin

Table des matières

Définition de la faille :

La faille Evil Twin (Jumeau Malveillant) est une technique de piratage de réseau sans fil qui consiste à créer une réplique d'un point d'accès WiFi légitime pour tromper les utilisateurs et les inciter à se connecter à un réseau malveillant. Lorsque les utilisateurs se connectent à cette réplique, les pirates peuvent voler des informations sensibles, comme des mots de passe ou des données de carte de crédit, ou encore rediriger les utilisateurs vers des sites web malveillants.

Exemple

Les attaques Evil Twin ont lieu la plupart du temps dans des lieux publiques. Admettons qu'une personne décide d'aller dans sa boulangerie préférée et s'assoie pour prendre un goûter. Iel se connecte au réseau wifi public le plus proche. Iel s'étaient déjà connecté à ce wifi avant donc iel ne suspecte rien. Mais en réalité une personne a réalisé un faux réseau wifi avec le même nom SSID. Etant donné qu'iel est proche de l'antenne malveillante sont signal est plus fort. Une fois connecté au wifi on prend notre billet de train en entrant nos coordonnées bancaires. Les données sont directement accessibles par la personne ayant installé le faux wifi.

Comment contrer une attaque Evil Twin ?

- Utiliser un réseau privé virtuel (VPN) pour chiffrer les données transmises lorsque vous vous connectez à un réseau WiFi public.
- Vérifiez toujours la sécurité du réseau WiFi avant de vous connecter (rechercher le nom du réseau et s'assurer qu'il est bien celui que vous voulez connecter).
- Utilisez un logiciel de sécurité pour vous protéger contre les réseaux malveillants.
- Utilisez un antivirus pour protéger votre appareil contre les logiciels malveillants.
- Utilisez des mots de passe forts et uniques pour vous connecter aux réseaux WiFi.
- Éviter de saisir des informations sensibles lorsque vous vous connectez à un réseau WiFi public.
- Il est important de noter qu'il est plus prudent d'utiliser sa propre connexion internet ou des réseaux WiFi sécurisés et connus pour éviter les risques d'attaque Evil Twin.

Voici quelques moyens techniques de contrer la faille Evil Twin:

- Utiliser des protocoles de sécurité pour les réseaux WiFi: Les protocoles de sécurité les plus couramment utilisés pour protéger les réseaux WiFi sont WPA et WPA2. Ces protocoles chiffrent les données transmises sur le réseau WiFi et utilisent des mots de passe forts pour protéger les réseaux contre les attaques Evil Twin.

- Utiliser des certificats de sécurité pour les réseaux WiFi: Les certificats de sécurité sont utilisés pour authentifier les points d'accès WiFi légitimes et protéger les réseaux contre les attaques Evil Twin. Les utilisateurs peuvent vérifier la validité d'un certificat en utilisant une autorité de certification de confiance.

- Utiliser des réseaux privés virtuels (VPN) pour se connecter à des réseaux WiFi publics: Les VPN chiffrent les données transmises sur les réseaux WiFi publics, protégeant ainsi les utilisateurs contre les attaques Evil Twin.

- Utiliser des outils de détection de réseau pour détecter les réseaux malveillants: Il existe des outils de détection de réseau qui peuvent détecter les réseaux malveillants, comme les réseaux Evil Twin, et alerter les utilisateurs. Ces outils peuvent être intégrés aux systèmes d'exploitation ou à des logiciels de sécurité.

- Utiliser des logiciels de sécurité pour protéger les appareils contre les logiciels malveillants: Les logiciels de sécurité peuvent protéger les appareils contre les logiciels malveillants qui peuvent être utilisés pour créer des réseaux Evil Twin ou voler des informations sensibles.

- Utiliser des réseaux WiFi sécurisés et connus : Il est plus prudent d'utiliser sa propre connexion internet ou des réseaux WiFi sécurisés et connus pour éviter les risques d'attaque Evil Twin.

Il est important de noter que ces moyens de contrer la faille Evil Twin ne sont efficaces que si elles sont correctement configurées et utilisées. Il est donc important de maintenir une bonne sécurité de ses appareils, réseaux et protocoles pour éviter les attaques Evil Twin.

Présentation d'un WIPS :

WIPS signifies : Wireless Intrusion Prevention System

Un WIPS sert à sécuriser un service Wifi et de détecter des points d'accès illégitimes, voisins. Ils permettent aussi de contrer les attaques en envoyant des trames de dissociation. En effet un WIPS est composé de trois éléments :

- Un système radio permettant d'écouter le trafic. Dans la plupart des cas, cette fonction est gérée directement par le point d'accès WiFi ;
- Le serveur de management, permettant de stocker l'ensemble des données ;
- La console de management, permettant à l'utilisateur d'avoir une interface facile d'utilisation. Cette interface peut se présenter sous la forme d'un outil dédié ou encore d'un portail web. La console et le serveur sont généralement gérés par le contrôleur/manager du réseau WiFi

Afin de prévenir ces attaques au mieux, les Wireless Intrusion Prevention System (WIPS) sont utilisés. Ce sont des systèmes permettant l'écoute radio et la reconnaissance de modèles d'attaques afin d'alerter l'administrateur du système de la menace.