Challenge 3 : Découvrir un mot de passe Wifi

Préambule

L'activité proposée est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains réseaux Wifi afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Il convient de rappeler que l'écoute d'un réseau WIFI ne peut se faire sans l'accord explicite de son propriétaire.
Tenter de casser la clé de chiffrement d'un réseau sans autorisation du propriétaire du réseau est un acte illégal et entraine votre responsabilité pénale.

La plupart des points d'accès sont configurés avec une clé de chiffrement suffisamment complexe pour considérer le réseau WIFI comme sécurisé.
Modifier la clé de chiffrement proposée par défaut peut rendre vulnérable votre réseau WIFI.

Objectifs

- Sonder les réseaux Wifi et les postes connectés
- Forcer un client à se reconnecter
- Capturer l'échange entre un client et une borne Wifi
- Tenter de déchiffrer le mot de passe Wifi

Logiciels

Vous utiliserez une machine **Kali Linux** pour tester vos attaques.

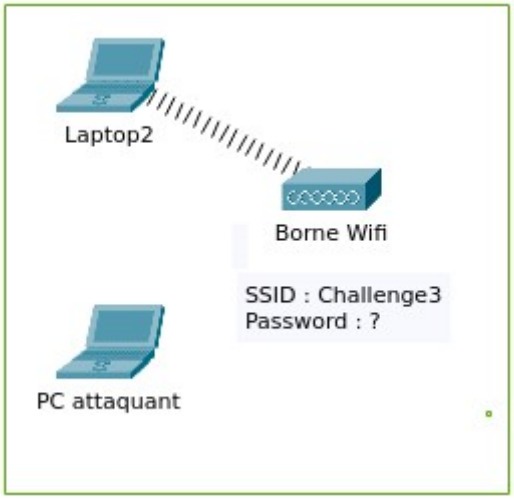
Aircrack-ng est une suite de logiciels de surveillance des réseaux sans fil dont l'utilisation principale est de « casser » les clés WEP et WPA des réseaux WIFI.

Scénario

Dans ce scénario, chaque groupe de travail utilisera une machine Kali **physique** (installée sur une clé USB/disque externe ou dual boot) pour tenter de découvrir le mot de passe du SSID « challenge3 ».

L'objectif est d'enregistrer une capture de trame sur le BSSID « challenge3 » et forcer un client à se déconnecter et à se reconnecter. Ainsi la poignée de main (handshak) sera capturée et pourra être analysée.

Le schéma du réseau est présenté ci-dessous :



Nous vous invitons à suivre les étapes suivantes :

1. Passer son interface WIFI en mode monitoriring
2. Analyser les paquets 802.11 et repérer les adresses mac du SSID informatique5 ainsi que d'un client connecté
3. Enregistrer une capture de trame sur le BSSID qui nous intéresse et forcer un client à se déconnecter et à se reconnecter
4. Découvrir le mot de passe en utilisant le dictionnaire rockyou.txt présent sur Kali