Sécurité informatique INF36207

Travail Pratique #4 – Expérimentation avec le WIFI

SESSION HIVER 2023

Date limite de remise du TP	25avril 2023 à 19h00
Équipe	Individuel ou en équipe de 2 ou 3 étudiants.
Pondération	15% (partie 1 + 2)

Mise en contexte

Vous venez d'être embauché dans une nouvelle entreprise et votre patron vous demande de faire le tour des installations et des systèmes et de lui revenir avec des recommandations afin d'améliorer la sécurité réseau de l'entreprise.

Vous devez expliquer à votre patron qui est un grand philosophe que la phrase qu'il a choisie pour sécuriser le réseau n'est pas très sécuritaire. Elle se retrouve déjà dans des dictionnaires de mots de passe qui sont largement disponibles sur Internet.

Vous devez lui prouver que sa phrase n'est pas sécuritaire en la cassant sans même la connaitre.

Travail à réaliser

Partie #1 :

Vous devez casser deux fois la clé WPA dont la capture du « handshake » a été réalisée dans le fichier **handshake-inf36207.cap** à l'aide du dictionnaire fourni. Les deux fichiers sont disponibles sur le portail.

Le cassage doit être fait par deux méthodes distinctes :

1. Cassure #1 : Utilisez l'outil ***hashcat***
    a. Notez que pour utiliser ***hashcat***, il y aura une étape intermédiaire nécessaire à la conversion du fichier au format *.cap* en un fichier compatible au format *.hccapx*.

2. Cassure #2 : Utilisez l'outil ***aircrack-ng***

Les deux expériences peuvent être réalisées à partir de votre machine Kali linux distribuée en classe.

Pour y arriver, vous devez faire vos propres recherches et apprendre d'avantages sur le fonctionnement des outils ***hashcat*** et ***aircrack-ng***. Vous pouvez vous consulter les références web données plus bas, ou encore faire vos propres recherches sur internet.

Partie #2 :

Vous devez décomposer et comprendre la commande WIFITE que nous avons utilisée en classe.

sudo wifite --verbose --kill -mac --showb --showm --nodeauths -ab

A. **--verbose**
B. **--kill**
C. **-mac**
D. **--showb**
E. **--showm**
F. **--nodeauths**
G. **-ab**

1. Identifier l'utilité de chacune des options saisies précédemment (points A à G) ?

2. Quelle serait l'option à passer à l'outil pour choisir un autre dictionnaire plutôt que celui par défaut ?

Références

- Liens sur WIFITE :
  - https://www.kali.org/tools/wifite/
  - https://github.com/kimocoder/wifite2
  - https://manpages.org/wifite
- Liens sur Aircrack-ng :
  - https://www.aircrack-ng.org/
  - https://github.com/aircrack-ng/aircrack-ng
  - https://manpages.org/aircrack-ng
- Liens sur Hashcat :
  - https://hashcat.net/hashcat/
  - https://github.com/hashcat/hashcat
  - https://manpages.org/hashcat

Livrables pour l'évaluation du travail pratique

Pour que votre travail pratique puisse être évalué par l'enseignant, vous devez déposer un document en format PDF contenant les éléments suivants :

- Fournir les réponses aux questions de la section #1
  - Inclure des captures d'écran en appui aux deux piratages de mots de passe réalisés;
- Fournir les réponses aux questions de la section #2
- Votre conclusion sur le piratage des réseaux sans-fil fait en classe, la sécurité des réseaux sans fil et une proposition de piste de sécurisation plus avancés qui pourrait être implantée.