Année 2023-2024

SAÉ Cyber 4.0 Sécurisation d'un SI

Tâche 6 Attaque sur le Wifi (4,5 points)

Liste des personnes impliquées avec pourcentage de répartition	
Sami	100%

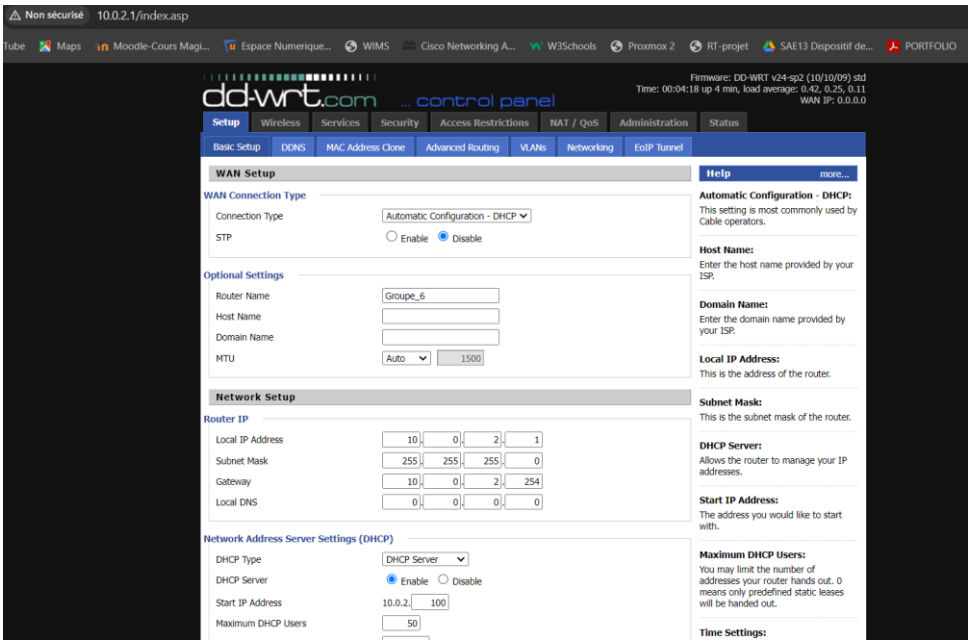
Estimation du temps passé sur cette tâche en heure-homme :

Objectif : Mettre en place des attaques sur le WEP et sur le WPA avec une Linksys puis avec un SNS

Mise en place du WEP sur Linksys :

Le WEP (Wired Equivalent Privacy) est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil, notamment les réseaux Wi-Fi. Il a été introduit initialement dans la norme IEEE 802.11 pour fournir une sécurité similaire à celle des réseaux filaires. Le but principal du WEP est de crypter les données transmises sur le réseau sans fil afin d'empêcher toute interception non autorisée.

Cependant, le WEP a été critiqué pour ses faiblesses de sécurité. Il utilise un algorithme de chiffrement relativement faible qui peut être facilement compromis avec des attaques telles que l'attaque par force brute ou l'attaque par paquets cryptographiques. En conséquence, le WEP est largement considéré comme obsolète et non sécurisé. De nos jours, il est recommandé d'utiliser des protocoles de sécurité plus robustes comme WPA (Wi-Fi Protected Access) ou WPA2 pour sécuriser les réseaux Wi-Fi.

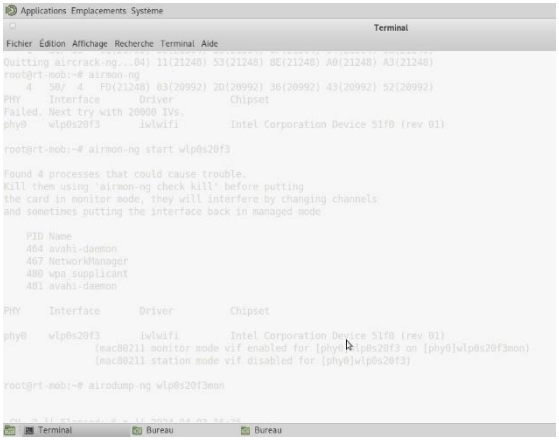


J'ai tout d'abord commencé par la configuration de l'adresse IP de notre borne lynksys en le configurant par rapport à notre schéma réseau. Pour cela, je suis allé dans la section 'Setup', puis 'Router IP'. Enfin j'ai changé le SSID du routeur en le nommant Groupe_6 pour pouvoir l'identifier parmi les autres.

Pour mettre en place un mot de passe tout en utilisant le protocole de sécurité WEP, il faut se rendre dans la section « Wireless » de l'interface de configuration du routeur. Suite à cela il faut se rendre dans l'onglet « Wireless Security ». Dans « Security Mode », j'ai sélectionné la partie « WEP ». Le fait d'avoir sélectionné ce protocole, a permit de pouvoir sélectionner plusieurs réglages tels que la génération de clés et le « Default Transmit Key » et « Encryption » qui nous permettent respectivement de pouvoir choisir la clé qui servira de mot de passe de connexion, et la taille de cryptage de la clé de connexion. J'ai ensuite cliqué sur le bouton « Generate » pour créer automatiquement des clés WEP. J'ai choisi la première clé générée comme mot de passe principal, en m'assurant qu'elle corresponde au numéro de la 'Default Transmit Key' sélectionnée. Cela a permis de sécuriser le réseau en utilisant le protocole WEP, conformément aux spécifications de notre infrastructure réseau.

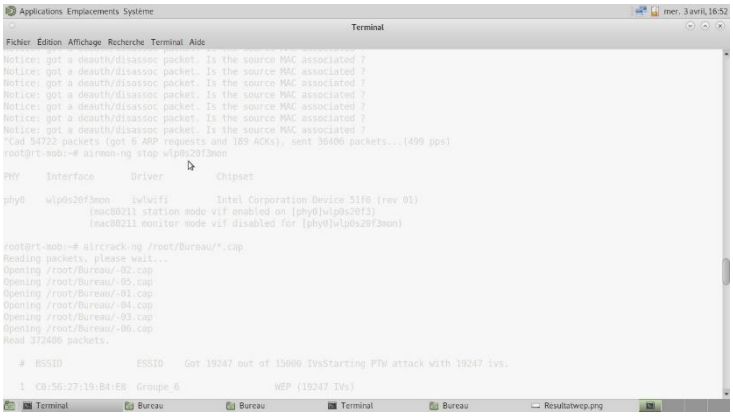
Cassage de la clé WEP sur linksys :

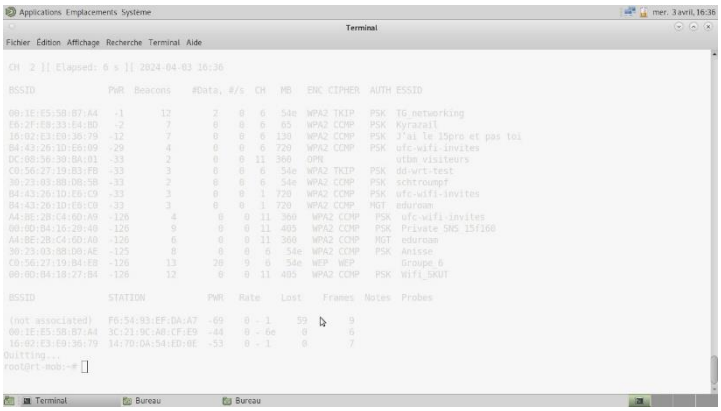
Pour débuter le processus de craquage d'un mot de passe WEP, j'ai utilisé le logiciel Aircrack-ng. J'ai lancé son installation sur mon système en exécutant la commande " apt-get install aircrack-ng" dans le terminal. Une fois le logiciel installé, j'ai utilisé la commande " airmon-ng" pour répertorier les interfaces réseau sans fil disponibles sur mon système. Cette étape était cruciale pour identifier l'interface que j'allais utiliser pour tenter de casser le mot de passe WEP.



Comme on peut le voir suite à cette commande, L'interface utilisée pour le réseau sans fil c'est à dire réseau wi fi est wlp0s20f3. Après avoir pris connaissance de l'interface utilisée, on va mettre par la suite en place le mois de moniteur qui est essentiel pour notre utilisation c'est à dire casser le mot de passe WEP. Ce dernier permet de surveiller tous les paquets de données qui circulent autour de nous.

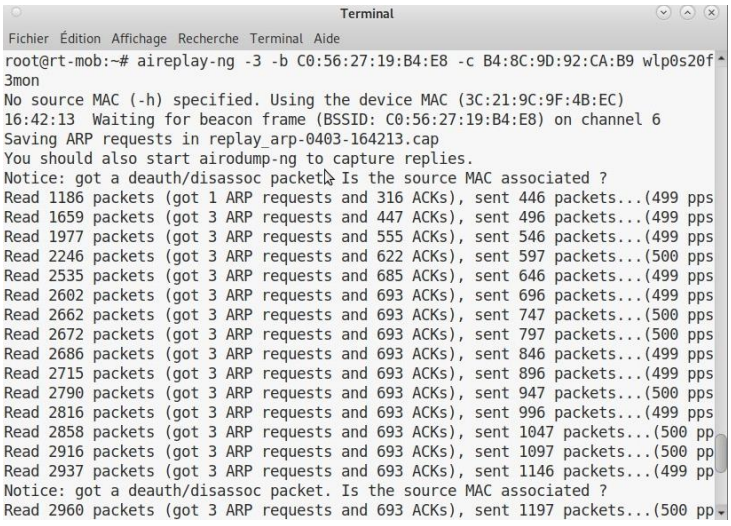
Suite à cela pour identifier la liste des réseaux wifi disponibles autour de nous j'ai tapé la commande airodump-ng wlp0s20f3mon. Cette liste contenait des données cruciales telles que le BSSID (adresse MAC du point d'accès), l'ESSID (nom du réseau), le canal utilisé par le réseau, ainsi que le type de sécurité mis en place pour chaque réseau. En me basant sur l'ESSID pour repérer les réseaux, j'ai identifié Groupe_6 comme le réseau cible pour lequel je voulais évaluer la sécurité WEP (qui est le wifi de notre routeur lynksys).



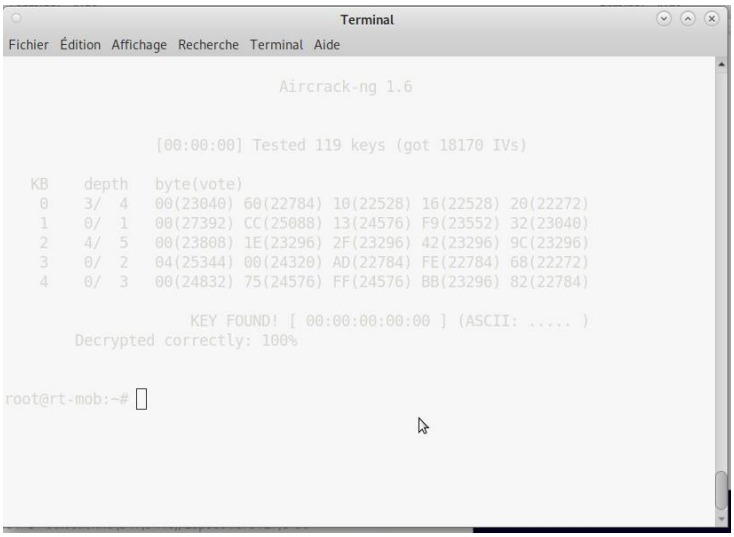


Suite à cela j'ai donc choisi le réseau cible avec son PC et j tapé la commande suivante qui me permet De voir quels appareils sont connectés à ce réseau et d'ainsi par la suite pouvoir capturer toutes les trames nécessaires pour craquer le mot de passe : airodump-ng -c 6 --bssid C0 :56 :27 :19 :B4 :E8 -w /home/tp/Bureau wlp0s20f3mon. Ici -c 6 signifie le canal de notre réseau. --bssid C0 :56 :27 :19 :B4 :E8 est l'identifiant de notre routeur sur le réseau, c'est grâce à cela que l'on va pouvoir récupérer les trames spécifiques à ce routeur. -w /home/tp/Bureau wlp0s20f3mon correspond à l'emplacement où nos données capturées seront enregistrées.

L'image ci-dessous correspond aux données capturées



Suites aux données capturées on stop la commande airmon-ng sur notre interface en mode moniteur et on lance le cassage de mode du wifi cible grâce à la commande aircrack-ng /home/tp/Bureau/*.cap. Ce qui nous donne ce résultat :

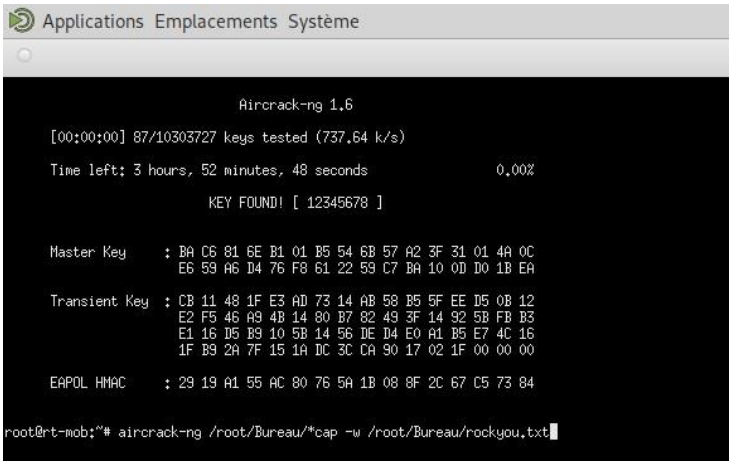


Mise en place du WPA :

Le WPA (Wi-Fi Protected Access) est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil Wi-Fi. Il offre un cryptage amélioré par rapport au protocole précédent, le WEP, ainsi qu'une authentification renforcée. Le WPA évolue continuellement pour améliorer la sécurité et est compatible avec les anciens équipements.

ci-dessus nous avons la configuration du WPA où l'on doit insérer une clé de connexion de notre choix.

Pour déchiffrer la clé pré-partagée WPA, j'ai suivi exactement le même protocole, à l'exception de la dernière étape où la commande "aircrack-ng" nécessitait l'utilisation d'un dictionnaire. J'ai donc créé un petit dictionnaire à cet effet. Voici la clé trouvée par le logiciel

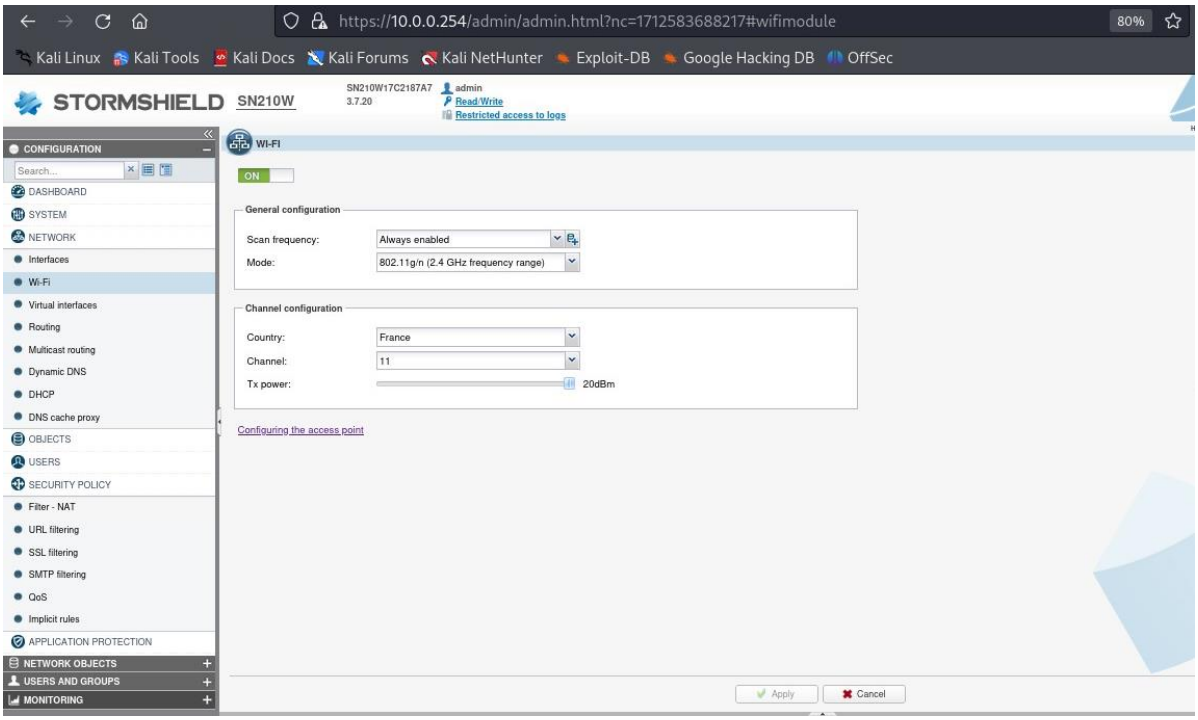


Normalement, le dictionnaire est généralement plus volumineux, ce qui entraîne des temps de craquage de mot de passe beaucoup plus longs. Si le mot de passe ne figure pas dans le dictionnaire, l'attaque échoue.

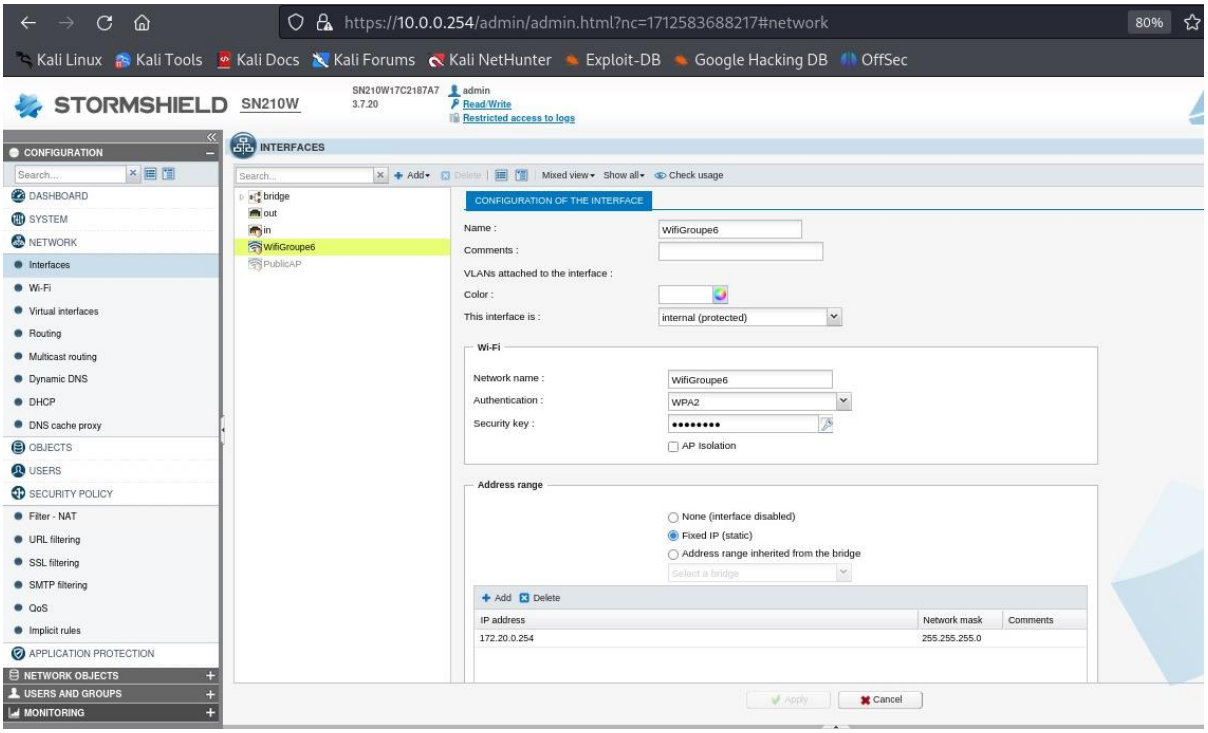
Mise en place du WPA sur Stormshield SNS :

NB : Il n'y a pas de WEP sur stormshield ainsi que WPA étant donné qu'il est affiché en tant que WPA2.

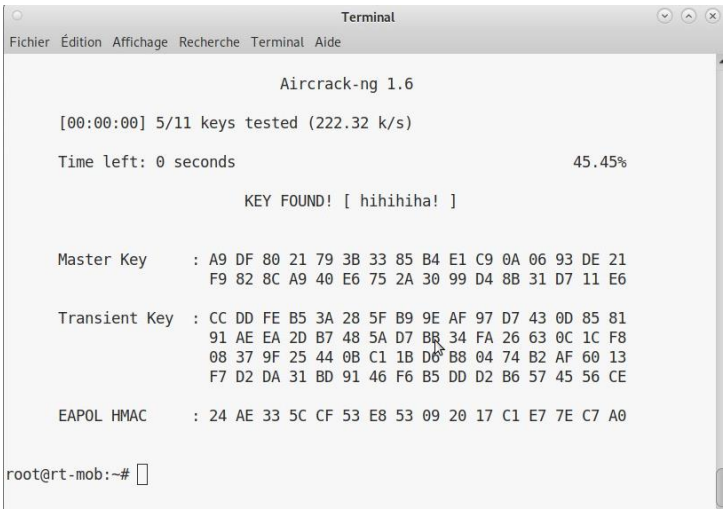
J'ai donc premièrement activé le wifi sur notre Stormshield B:



Puis j'ai activé l'interface wifi avec le chiffrement WPA2 :



La procédure est exactement la même que pour la WPA



Voici donc le résultat.