TP de Pentesting Ysoar

Compétences mises en œuvre : Gérer le patrimoine informatique,

Répondre aux incidents

Les failles et leurs solutions

Faille n°1 : le point d'entrée.

Suite à un mail de phishing envoyé à l'employé Arthur Dugard, avec une fausse adresse mail contenant le nom de domaine "Ennodis", demandant de nous indiquer son nom de compte dans le domaine informatique, celui-ci nous répondit le nom de compte "a.dugard", qui marquera le point d'entrée dans le système.

Grâce à une étude de ses réseaux sociaux et de ses posts, nous avons pu en déduire que son mot de passe était "Simba62" grâce à une attaque par force brute, et avons eu accès à son compte sur son poste de travail.

Solution n°1 :

Être vigilant sur les emails de phishing, bien vérifier le nom de domaine présent dans l'adresse mail et également utiliser un mot de passe bien plus **robuste**. (CF. les recommandations de L'ANSSI)

Afin de cracker le mot de passe du compte AdminLocal, nous avons utilisé le logiciel HashCat.

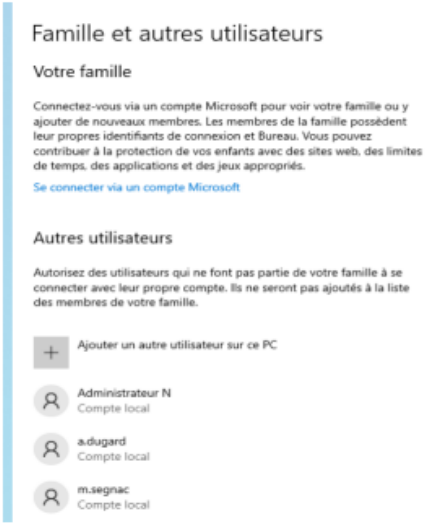
Grâce à HashCat, nous avons récupéré le mot de passe du compte AdminLocal, nous donnant pleinement accès au compte administrateur du poste.

Solution pour le compte AdminLocal :

Utiliser un mot de passe plus robuste, donnant beaucoup plus de difficultés aux logiciels de cassage et pouvant stopper ce type d'attaques. (CF Recommandations de l'ANSSI)

Faille n°4 : Sécurité organisationnelle compromise :

Maintenant que nous avons accès au compte administrateur, nous avons pu créer un nouveau compte de type administrateur sur le poste nommé “Administrateur N”



Solution : suivre toutes les recommandations de sécurité précédentes, afin d’éviter ce genre de situation.

Faille n°5 : Failles physiques:

Toutes ces intrusions informatiques ont pu être commises à cause de failles de sécurités physiques via du PiggyBacking.

Solution : Augmenter les sécurités physique du site de Béthune (agent de sécurité etc...)