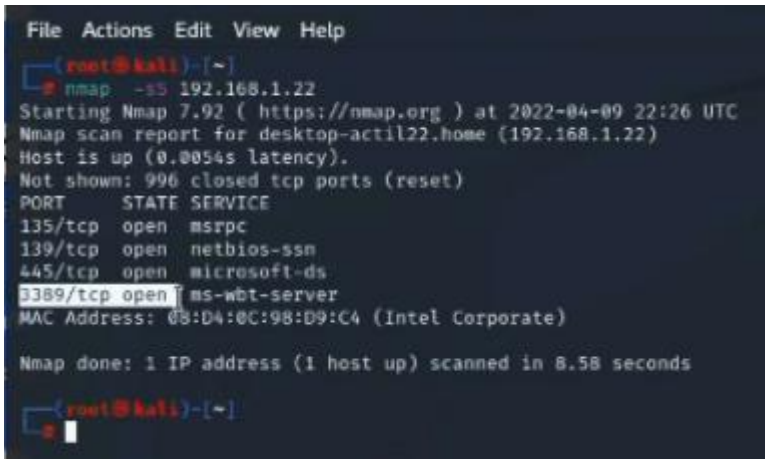
Attaque partage SMB + casser les crédencials sur Windows

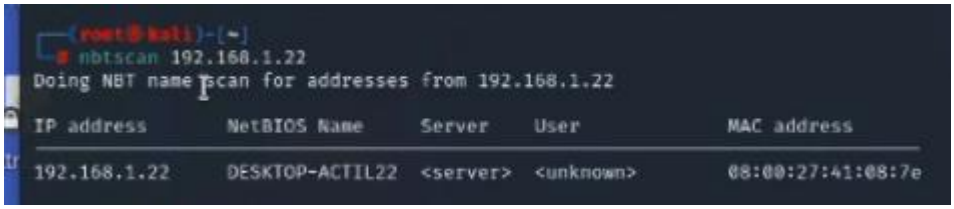
Tout d'abord sur la machine attaquante je réalise un scan sur la machine cliente avec

nmap -sS « ip machine »

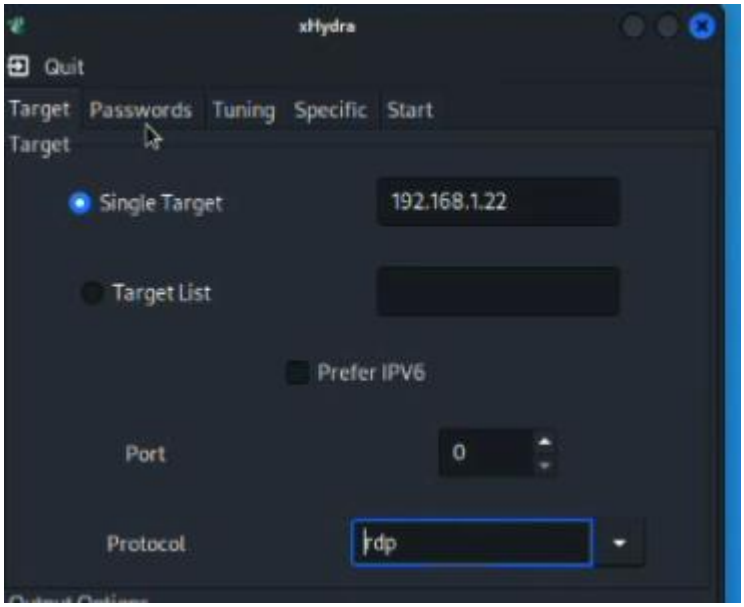



Nous pouvons que le port 3389 est ouvert

Je fais donc un nbtscan « ip machine » qui me donnera le nom de la machine

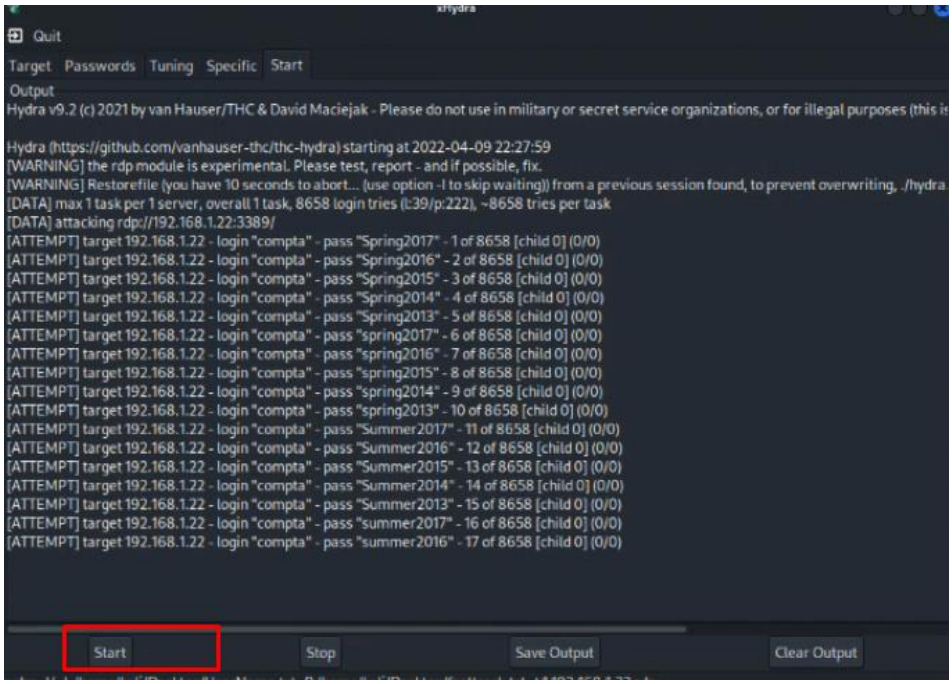



Ensuite nous allons utiliser le logiciel hydra qui existe en interface graphique nous allons renseigner l'ip de notre victime et le protocole sur lequel nous allons faire l'attaque

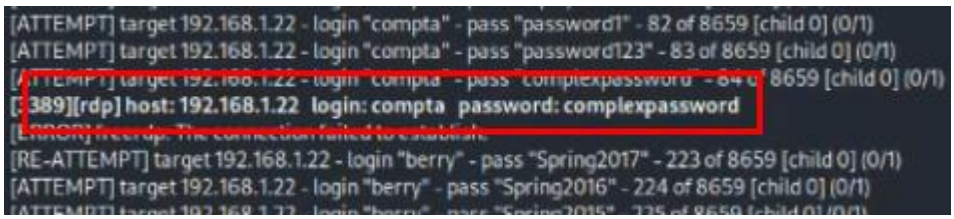


Ainsi que les différentes Word List téléchargées


Ensuite nous démarrons l'attaque dans l'onglet « start » nous pouvons voir que hydra fait une attaque par dictionnaire en testant tous les mots de passe sur le login compta.



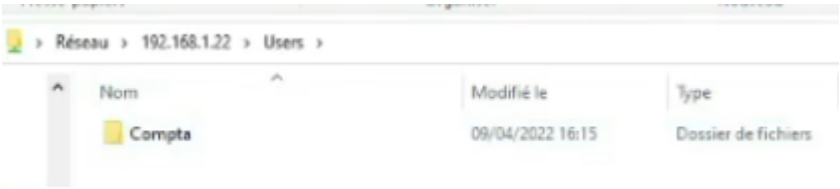

On peut voir qu'il fini par trouver le mot de passe mais continu a tester les mots de passe.



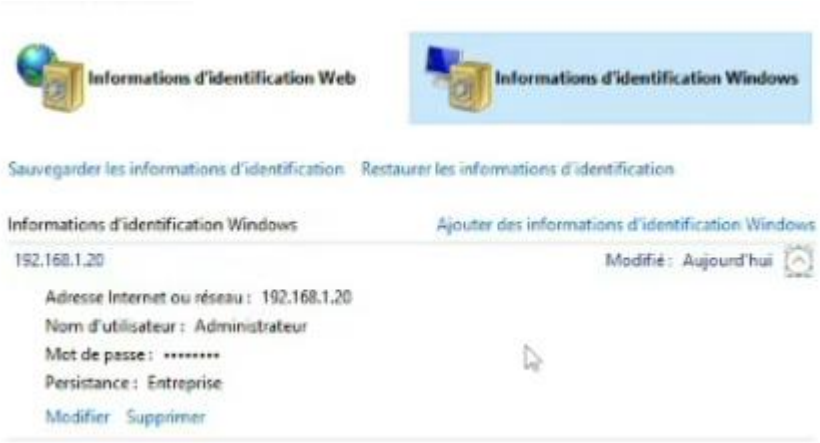

Donc le login est « compta » avec comme mot de passe « complexpassword »

La première étape est réalisée maintenant nous pouvons nous connecter à la machine et voir ce qu'elle réserve.

Nous avons donc accès au partage smb



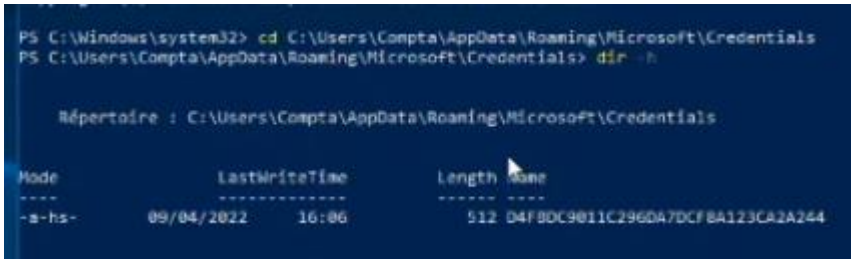

De plus le bureau à distance est configuré dessus nous pouvons voir que dans les credentials windows un Utilisateur « Adinistrateur » et son mot de passe est enregistré.



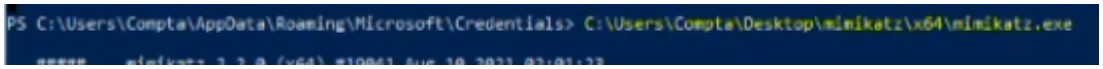

Nous allons donc casser le mot de passe des credentials car il n'est pas visible par l'utilisateur. Nous allons pour cela utiliser le logiciel mimikatz.

**Mimikatz** est un outil permettant d'effectuer diverses actions sur un système Windows : injection de bibliothèques, manipulation de processus, extraction de hashes et de mots de passe notamment.

Dans le dossier credentials en powershell nous pouvons voir un nom c'est ce nom qui va nous intéresser.



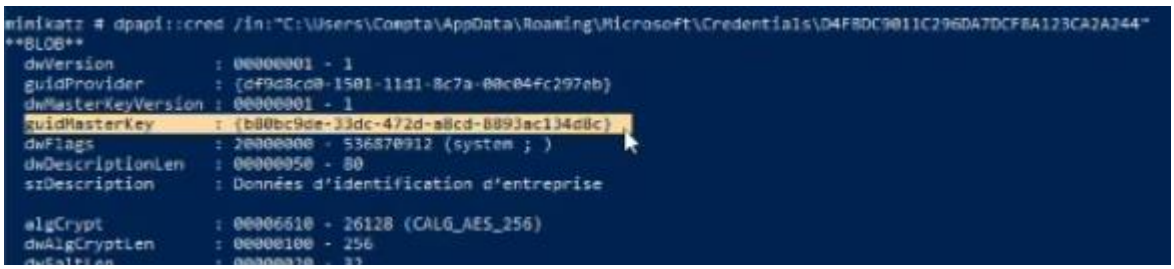

Ensuite nous allons lancer mimikatz



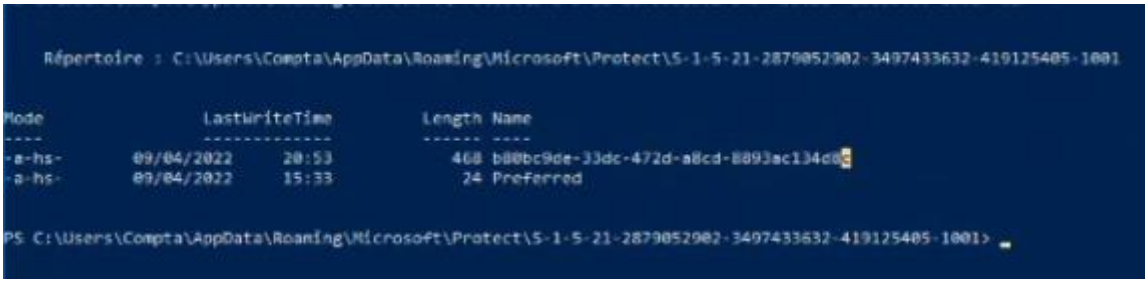

Puis nous allons augmenter nos privilèges avec la commande « privilege ::debug »

Ensuite nous allons taper la commande suivante donc le chemin suivi du nom du dossier ou se trouve les credentials.

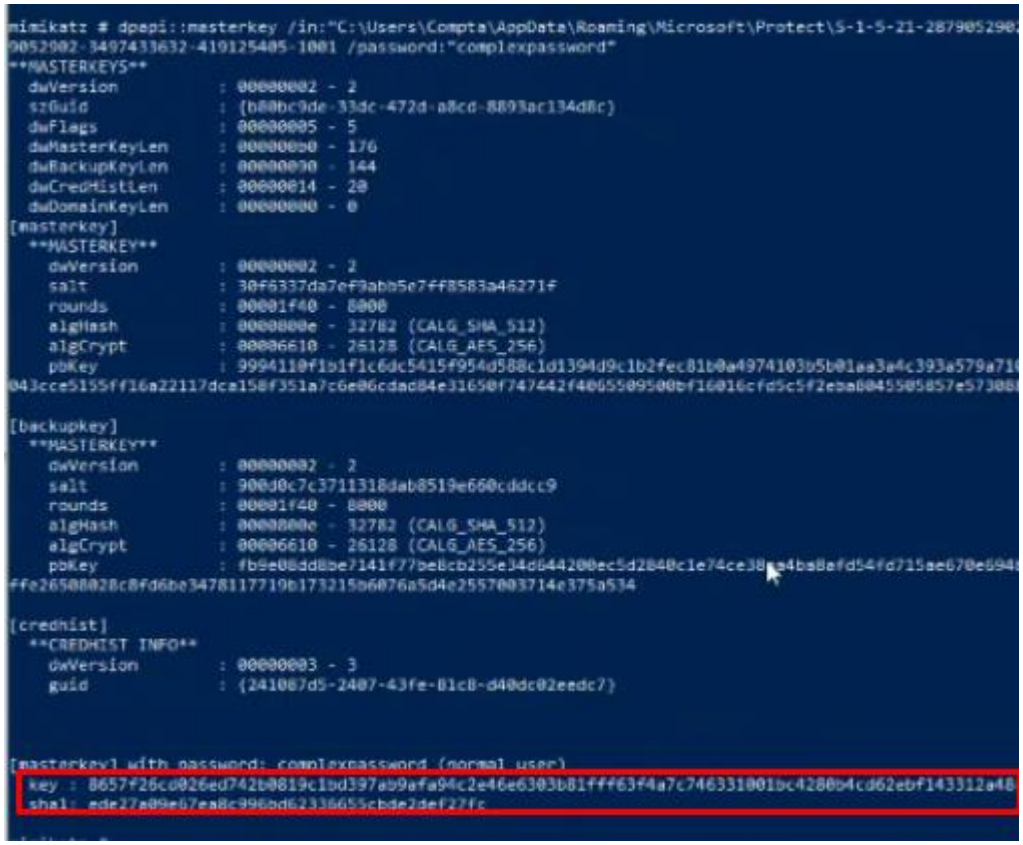

Cela nous permet de récupérer le GUIDmasterkey



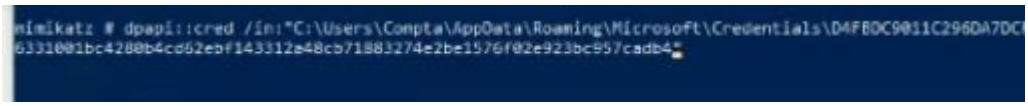

Ensuite dans le répertoire protect on récupère comme auparavant un om je precise que ce sont des fichier caché non visible dans l'explorateur de fichier même en affichant les fichiers cachés



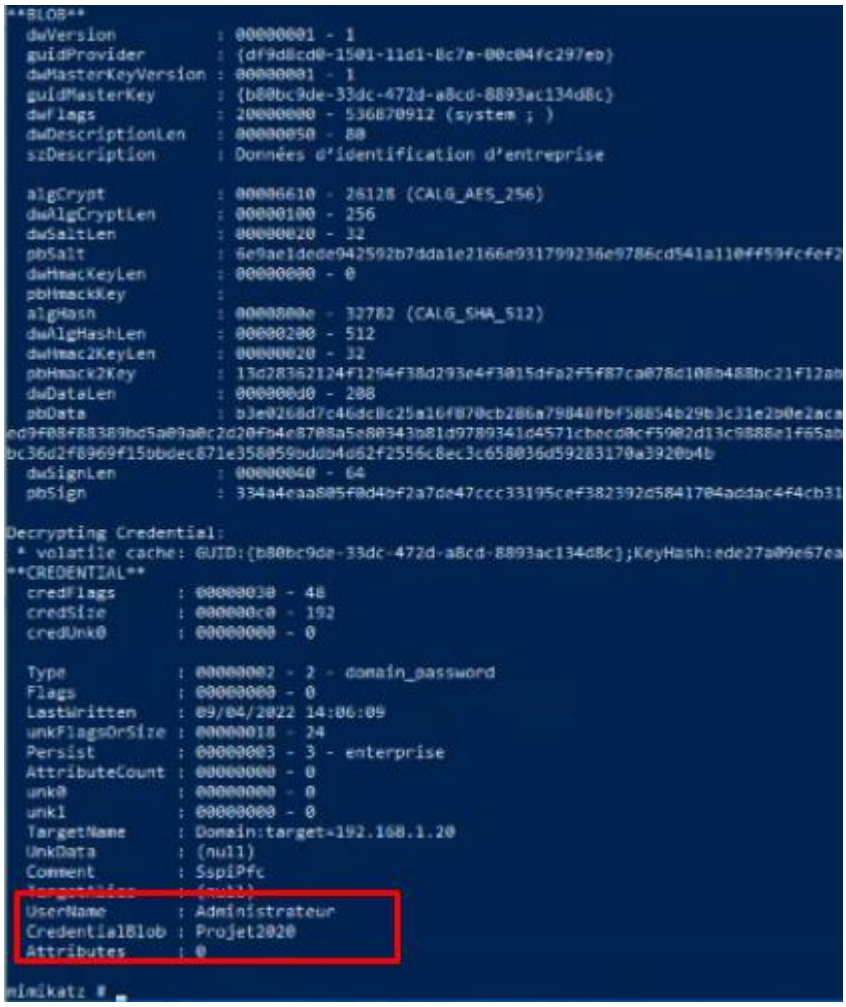

En tapant la commande suivante avec le protect name et le guid master key et en résignant le mdp de la session précédemment cassée nous obtenons la key



Ensuite avec la commande avec le nom credential suivi de la key




Nosus finissons par trouver le mot de passe « Projet2020 »




Connexion en shell au serveur :

Enter-PSSession -ComputerName « ipserveur » -Credential Administrateur

Cela nous ouvre une pop-up il faudra juste renseigner le mot de passe admin précédemment récupérer session shell avec le compte administrateur.