

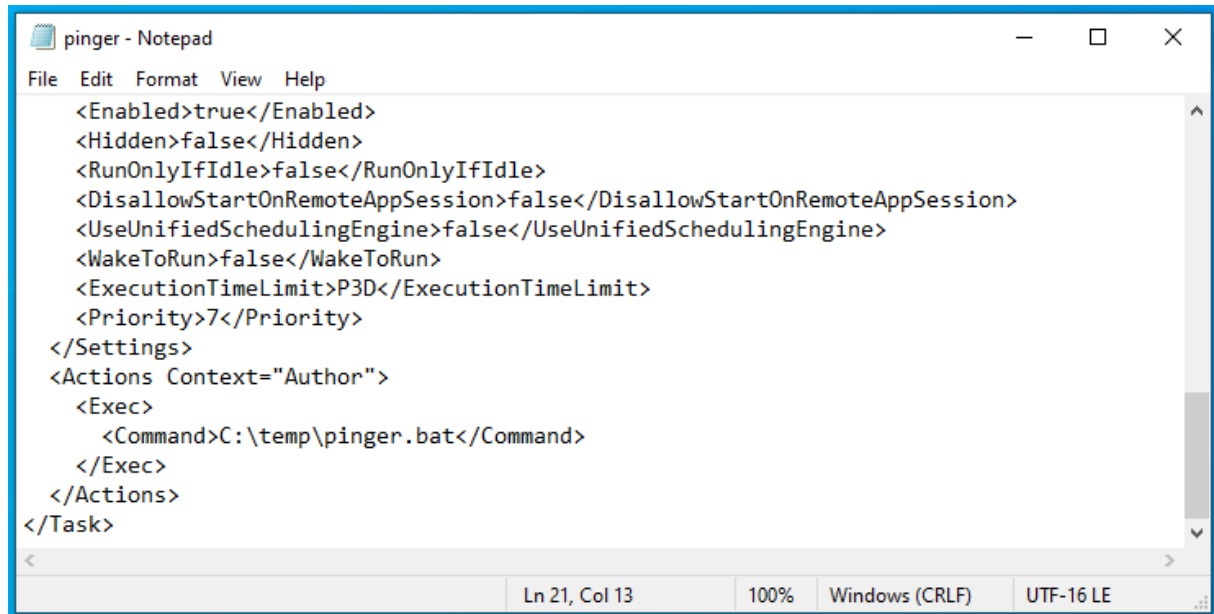
System Security

Practicum 1: Windows privilege escalation

1) Scheduled tasks

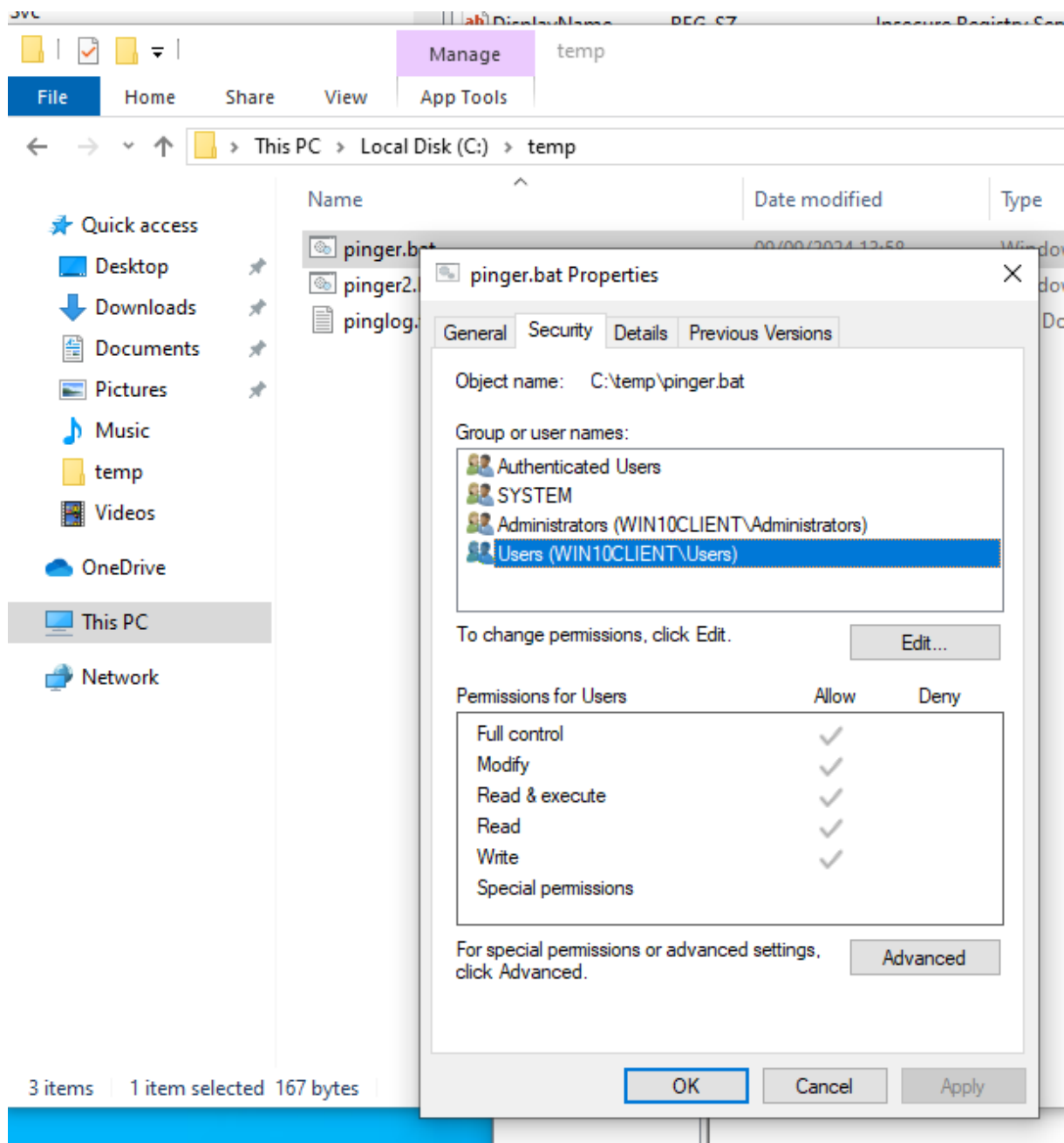
C:\Windows\Tasks Migrated

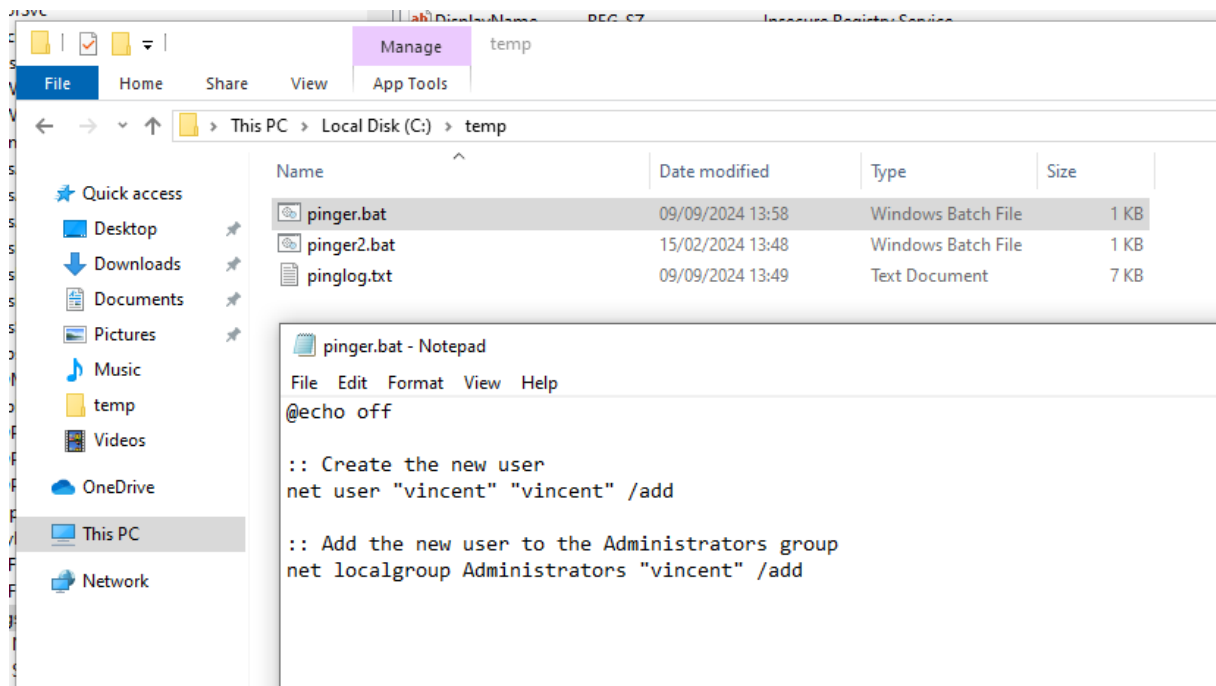
The pinger file contains at the end a option to execute a file:



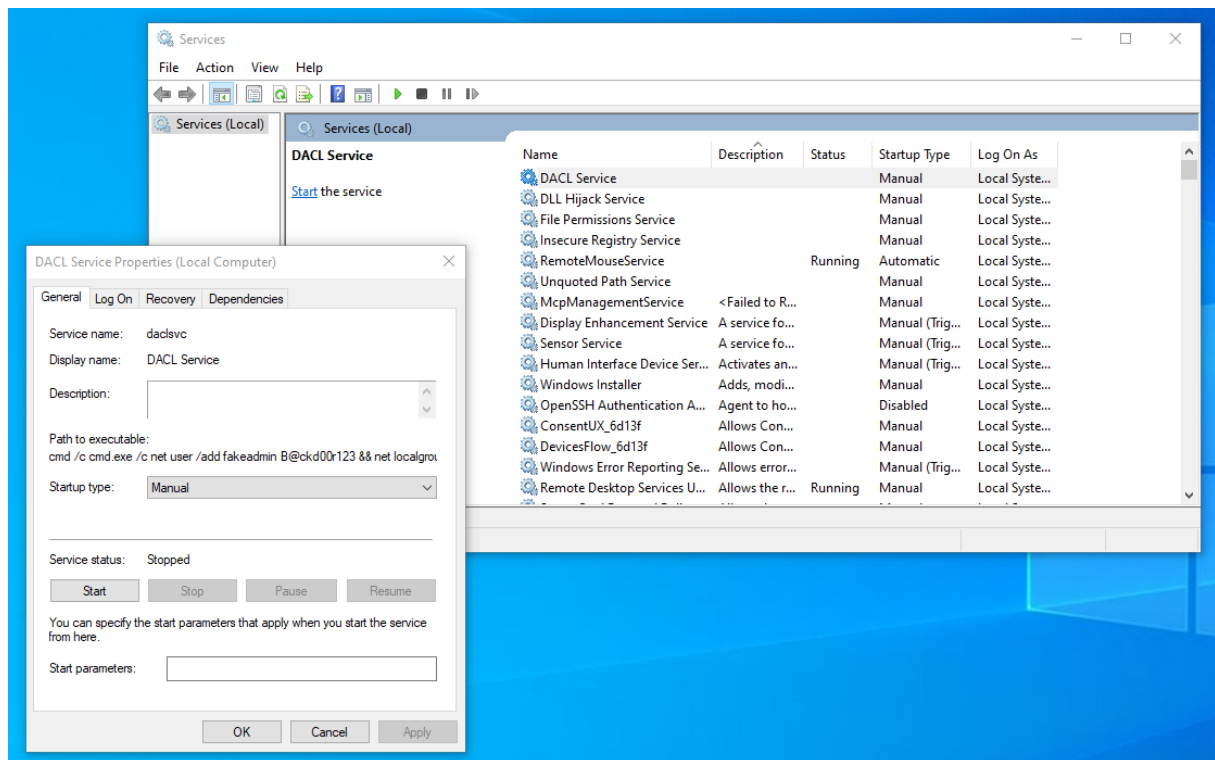
```
pinger - Notepad
File Edit Format View Help
<Enabled>true</Enabled>
<Hidden>false</Hidden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<DisallowStartOnRemoteAppSession>false</DisallowStartOnRemoteAppSession>
<UseUnifiedSchedulingEngine>false</UseUnifiedSchedulingEngine>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>P3D</ExecutionTimeLimit>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>C:\temp\pinger.bat</Command>
  </Exec>
</Actions>
</Task>
```

Ln 21, Col 13 100% Windows (CRLF) UTF-16 LE

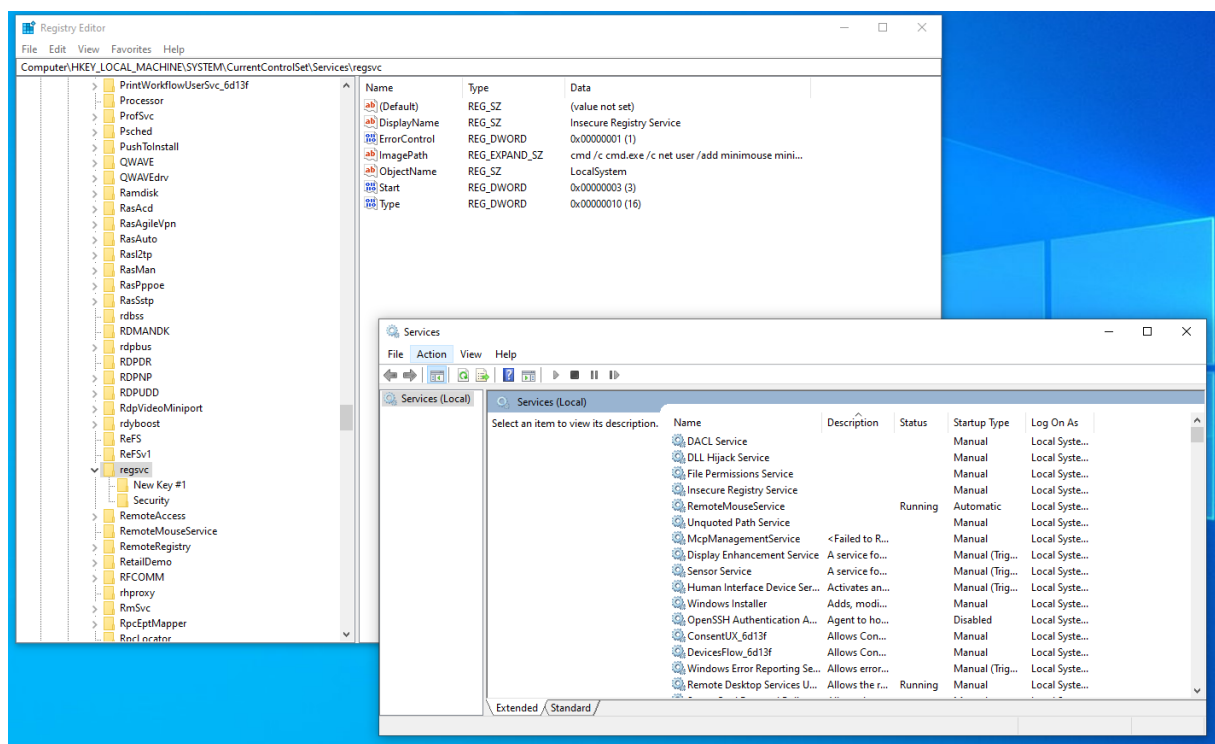





services.msc




regedit



5)

 **U**

Met welke commandline tool kan ik zien welke services unquoted services paths gebruiken

 **Copilot**

✓ Antwoorden voor u genereren...






Je kunt de **WMIC** (Windows Management Instrumentation Command-line) tool gebruiken om te controleren welke services onjuiste paden gebruiken. Hier is een commando dat je kunt uitvoeren in de command prompt (als administrator):

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

Dit commando zoekt naar services die automatisch starten en waarvan de paden niet correct zijn omgeven door aanhalingstekens ¹.

Heb je hulp nodig bij het uitvoeren van dit commando of bij het oplossen van eventuele gevonden problemen?

Meer informatie [1 isgovern.com](#) [2 attack.mitre.org](#) [3 dfirlab.org](#) [4 cisotimes.com](#) [+1 meer](#)

     1 van 10

Exclude C: drive via cmd.exe:

powershell -Command "Add-MpPreference -ExclusionPath 'C:\Temp'"

Kijken welke geexclude is:

powershell -Command "Get-MpPreference | Select-Object -ExpandProperty ExclusionPath"

