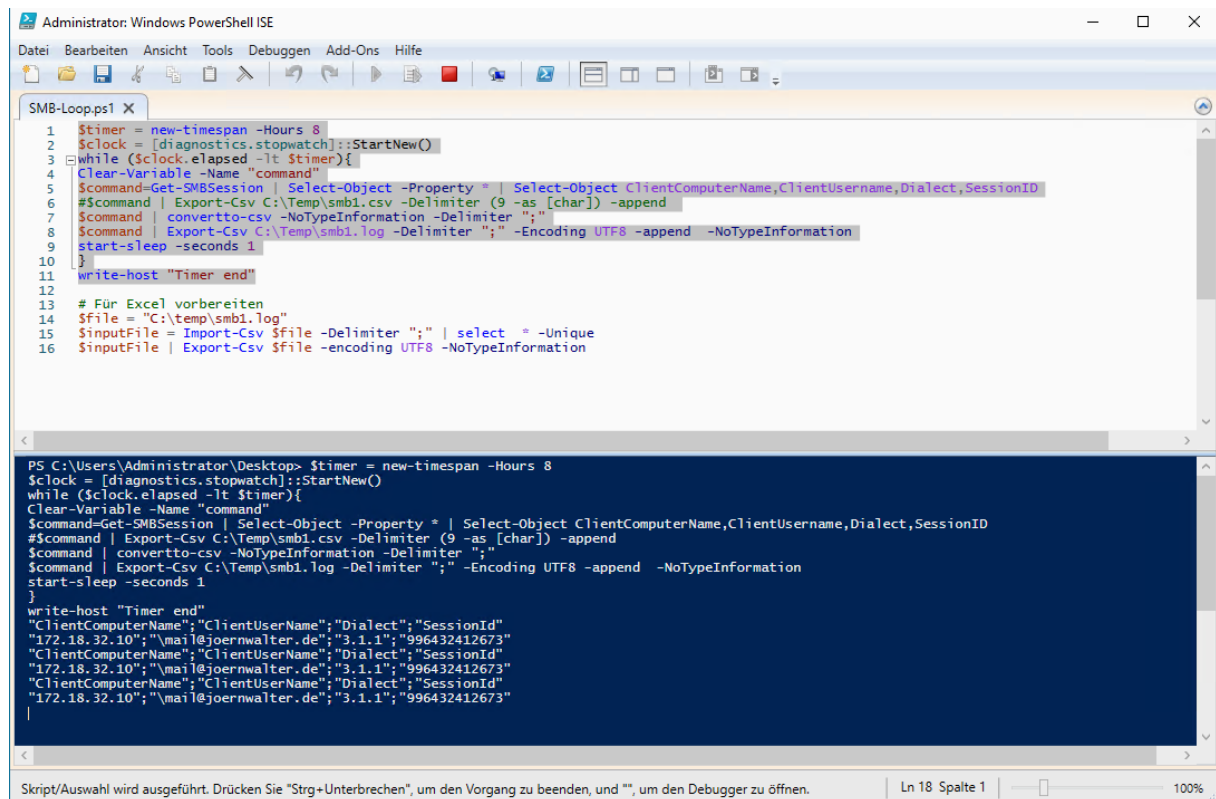


## SMBv1 - Monitoring

Mit diesem Skript loggen wir für eine definierte Zeit den Zugriff via SMB-Protokoll.

Nachdem das Skript gestartet wurde, sperrt man einfach den Bildschirm.



The screenshot shows the Windows PowerShell ISE interface. The script 'SMB-Loop.ps1' is open in the editor. The script defines a timer for 8 hours and a stopwatch to track execution. It enters a loop that runs while the stopwatch is less than the timer. Inside the loop, it clears a variable named 'command', gets SMB session information, and exports it to a CSV file. The output of the script is shown in the console window, displaying the session information for the first iteration.

```

1 $timer = new-timespan -Hours 8
2 $clock = [diagnostics.stopwatch]::StartNew()
3 while ($clock.elapsed -lt $timer){
4     Clear-Variable -Name "command"
5     $command=Get-SMBSession | Select-Object -Property * | Select-Object ClientComputerName,ClientUsername,Dialect,SessionID
6     # $command | Export-Csv C:\Temp\smb1.csv -Delimiter (9 -as [char]) -append
7     $command | convertto-csv -NoTypeInformation -Delimiter ";"
8     $command | Export-Csv C:\Temp\smb1.log -Delimiter ";" -Encoding UTF8 -append -NoTypeInformation
9     start-sleep -seconds 1
10 }
11 write-host "Timer end"
12
13 # Für Excel vorbereiten
14 $file = "C:\temp\smb1.log"
15 $inputFile = Import-Csv $file -Delimiter ";" | select -Unique
16 $inputFile | Export-Csv $file -encoding UTF8 -NoTypeInformation
    
```

```

PS C:\Users\Administrator\Desktop> $timer = new-timespan -Hours 8
$clock = [diagnostics.stopwatch]::StartNew()
while ($clock.elapsed -lt $timer){
Clear-Variable -Name "command"
$command=Get-SMBSession | Select-Object -Property * | Select-Object ClientComputerName,ClientUsername,Dialect,SessionID
# $command | Export-Csv C:\Temp\smb1.csv -Delimiter (9 -as [char]) -append
$command | convertto-csv -NoTypeInformation -Delimiter ";"
$command | Export-Csv C:\Temp\smb1.log -Delimiter ";" -Encoding UTF8 -append -NoTypeInformation
start-sleep -seconds 1
}
write-host "Timer end"
ClientComputerName;"ClientUsername";"Dialect";"SessionId"
"172.18.32.10";"mail@joernwalter.de";"3.1.1";"996432412673"
ClientComputerName;"ClientUsername";"Dialect";"SessionId"
"172.18.32.10";"mail@joernwalter.de";"3.1.1";"996432412673"
ClientComputerName;"ClientUsername";"Dialect";"SessionId"
"172.18.32.10";"mail@joernwalter.de";"3.1.1";"996432412673"
    
```

```

$timer = new-timespan -Hours 8
$clock = [diagnostics.stopwatch]::StartNew()
while ($clock.elapsed -lt $timer){
Clear-Variable -Name "command"
$command=Get-SMBSession | Select-Object -Property * | Select-Object
ClientComputerName,ClientUsername,Dialect,SessionID
# $command | Export-Csv C:\Temp\smb1.csv -Delimiter (9 -as [char]) -append
$command | convertto-csv -NoTypeInformation -Delimiter ";"
$command | Export-Csv C:\Temp\smb1.log -Delimiter ";" -Encoding UTF8 -append -
NoTypeInformation
start-sleep -seconds 1
}
write-host "Timer end"
    
```

## SMBv1 - Monitoring

Das Ergebnis mit welcher Protokollversion der Zugriff stattfand ist ausschlaggebend für die Deaktivierung bzw. der weiteren Prüfung.

Das Log sagt aus, dass der Zugriff nur mit der SMB-Protokollversion 3.11 stattfand.

[illegible]

Somit kann SMBv1 ohne Sorge deaktiviert bzw. deinstalliert werden.

## SMBv1 - Monitoring

Die Ausgabe für Excel etwas verschönern. Doppelte Einträge werden entfernt und alles schön mit Semikolon getrennt.

```
# Für Excel vorbereiten
$file = "C:\temp\smb1.log"
$inputFile = Import-Csv $file -Delimiter ";" | select * -Unique
$inputFile | Export-Csv $file -encoding UTF8 -NoTypeInfo
```



<https://www.der-windows-papst.de/2021/05/27/smb-dialect-revision-konfigurieren/>