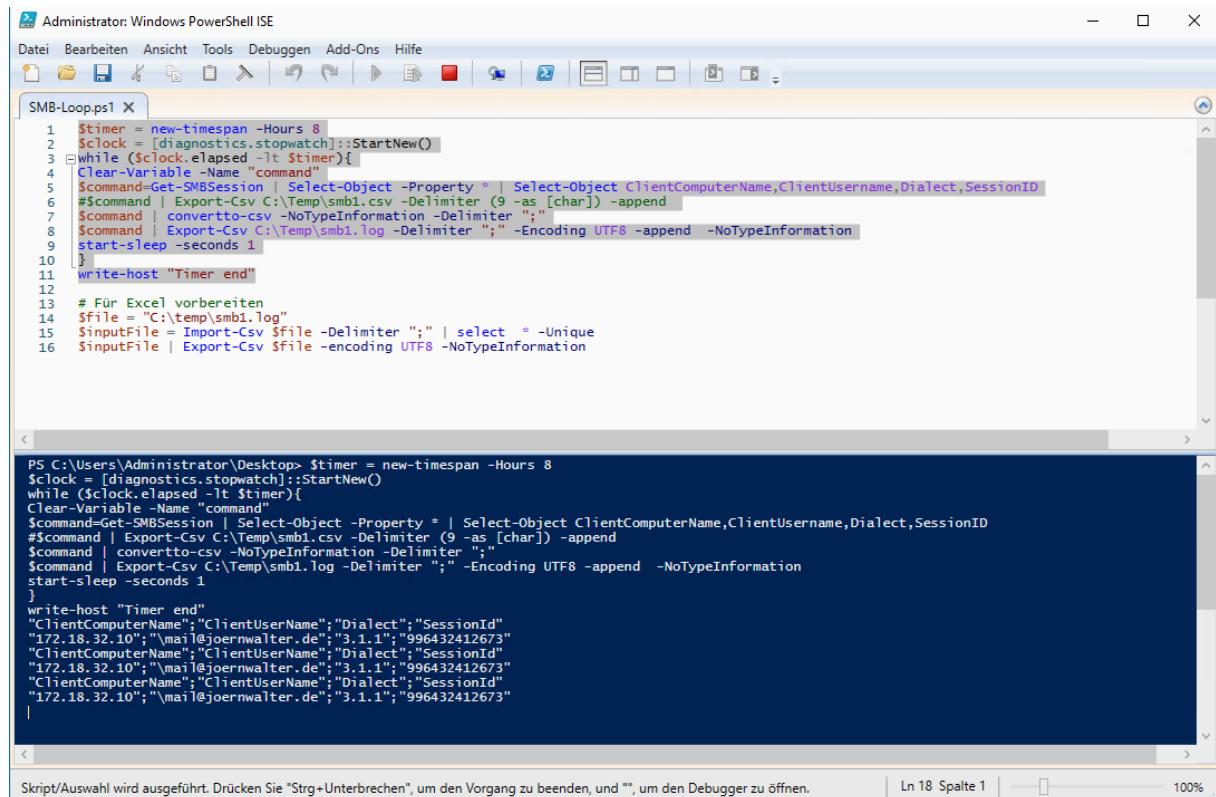


## SMBv1 - Monitoring

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

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



```

Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
SMB-Loop.ps1
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"
|
```

Skript/Auswahl wird ausgeführt. Drücken Sie "Strg+Unterbrechen", um den Vorgang zu beenden, und "", um den Debugger zu öffnen. | Ln 18 Spalte 1 | 100%

```

$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, das der Zugriff nur mit der SMB-Protokollversion 3.11 stattfand.

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 -NoTypeInformation
```



The screenshot shows a Windows Notepad window with the title 'smb1.log - Editor'. The window contains a single line of CSV data: 'ClientComputerName;""ClientUserName"";""Dialect"";""SessionId""' followed by the IP address '172.18.32.10;""\mail@joernwalter.de"";""3.1.1"";""996432412673""'. The Notepad window has a standard Windows interface with a menu bar (Datei, Bearbeiten, Format, Ansicht, Hilfe), status bar (Zeile 1, Spalte 1, 100%, Windows (CRLF), UTF-8), and scroll bars.

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