Port Scanning in Windows

We will use the Test-NetConnection cmdlet for that.

Test-NetConnection is a PowerShell cmdlet that displays diagnostic information for a network connection. It supports various tests, including ping, TCP connection, route tracing, and route selection diagnostics

```
# Use Test-Connection script in Windows. Status "True" indicates open port

PS C:\> Test-NetConnection -Port 445 192.168.50.151
```

```
# Powershell one liner for port scan on 1-1024 ports

PS C:\> 1..1024 | % {echo ((New-Object
Net.Sockets.TcpClient).Connect("192.168.50.151", $_)) "TCP port $_ is
open"} 2>$null
```
