Lateral Movement Admin -> System

> **Lateral movement** refers to the techniques that cyber attackers, or threat actors, use to progressively move through a network as they search for the key data and assets that are ultimately the target of their attack campaigns.[1][2][3] While development of more sophisticated sequences of attack has helped threat actors develop better strategies and evade detection as compared to the past, similar to planning a heist, cyber defenders have also learned to use lateral movement against attackers in that they use it to detect their location and respond more effectively to an attack.[1]

Lateral movement (cybersecurity) - Wikipedia

PSexec Alternativen

wenn es bereits bestehende Sicherheitsmaßnahmen gibt, wie z.B. den Aufruf von \\live.sysinternals.com\tools\psexec64.exe zu verhindern.

```
schtasks /create /tn RunAsSystem /tr "cmd.exe /c your_command" /sc once /st 00:00 /ru SYSTEM /f
```

- Impacket -> psexec.py & smbexec.py - SMBexec soll weniger AV triggern...

```
Enable-PSRemoting
$sess = New-PSSession -ComputerName <Name>
Enter-PSSession -ComputerName <Name> OR -Sessions <SessionName>
```

Drittanbieter

- Windows Lateral Movement with smb, psexec and alternatives | nv2lt - Scratching the Surface
- GitHub - S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet: A cheat sheet that contains common enumeration and attack methods for Windows Active Directory.

Version #7
Erstellt: 2024-08-12 11:41:25 UTC von Konstantin
Zuletzt aktualisiert: 2024-08-12 12:07:11 UTC von Konstantin