PowerShell Conference Europe

Next Up:

Evgenij Smirnov

Antwerp 24

3

2

1

PowerShell Conference Europe

Connecting to Systems in a trustless world…

Evgenij Smirnov

Antwerp 24

Many thanks to our sponsors:

PATCH MY PC

semperis

ScriptRunner®
Your #1 for PowerShell Automation

@cj_berlin

Evgenij Smirnov

```
PS C:\> Get-SpeakerInfo

Name         : Evgenij Smirnov
Twitter      : @cj_berlin
BlogSite     : https://it-pro-berlin.de
Location     : Berlin
YearOfBirth  : 1972
JobTitle     : Senior Solutions Architect
WorksAt      : Semperis
MVPSince     : 2020
UserGroups   : {WSUG, EXUSG, PSUGB}
SpokeAt      : {PSConfEU, CIMLingen, PSConfEU, PSDAY.UK…}
CertifiedIn  : {Microsoft, VMware, Quest, ITIL}
```

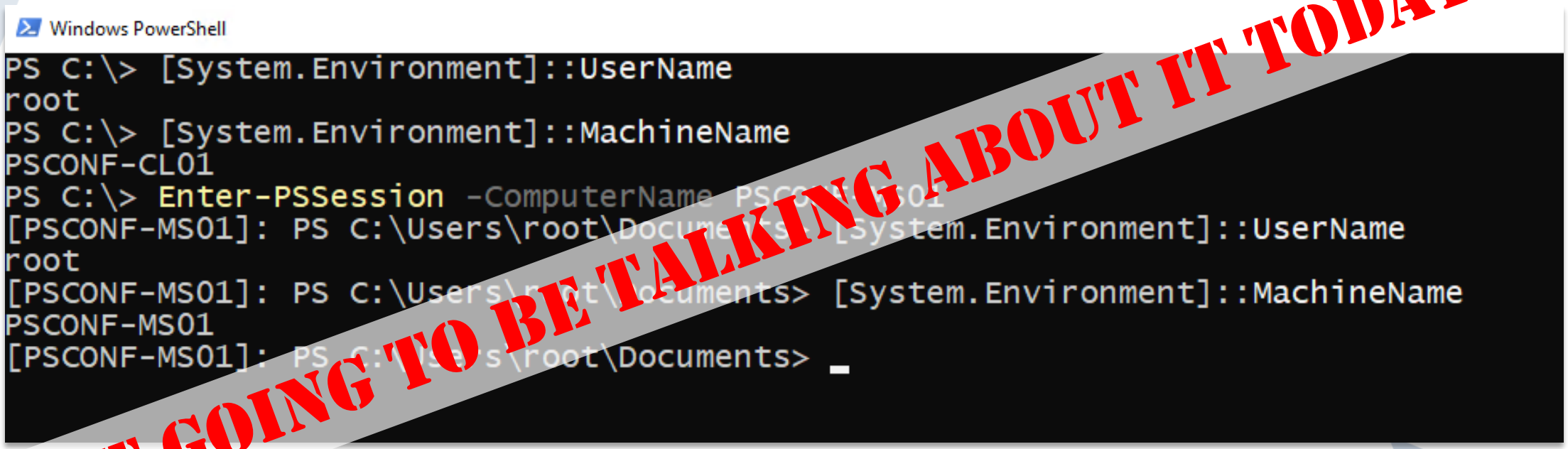
Microsoft® MVP Most Valuable Professional

@cj_berlin

In this session…

- Things we don‘t ~~want~~ have to talk about…
- Things we want to talk about…
- Things they don‘t want us to talk about…
- And other stuff ☺

PSRemoting was made for…



@cj_berlin

PS 7.3+ allows custom transports

- Can use whatever technology underneath
- Can utilize own authentication and authorization
- Jordan Borean talked about it yesterday
- Justin Grote talked about it last year
- Could be the future of trust-free remoting

NOT GOING TO BE TALKING ABOUT IT TODAY

In an untrusted world…

- workgroup deployments of Tier 0 systems
  - Backup
  - Monitoring
  - Config management
- cross-platform automation
  - e.g. agentless security configuration scans
- …still have to manage it all somehow ☺

In an untrusted world…

- No implicit trust
  - standalone systems or non-trusting security realms
  - source machine must be standalone
  - target machine must be standalone
  - DNS resolution may or may not be available
- Hardened attack surface
  - open ports / enabled protocols
  - configuration permissions

Living Off the Land

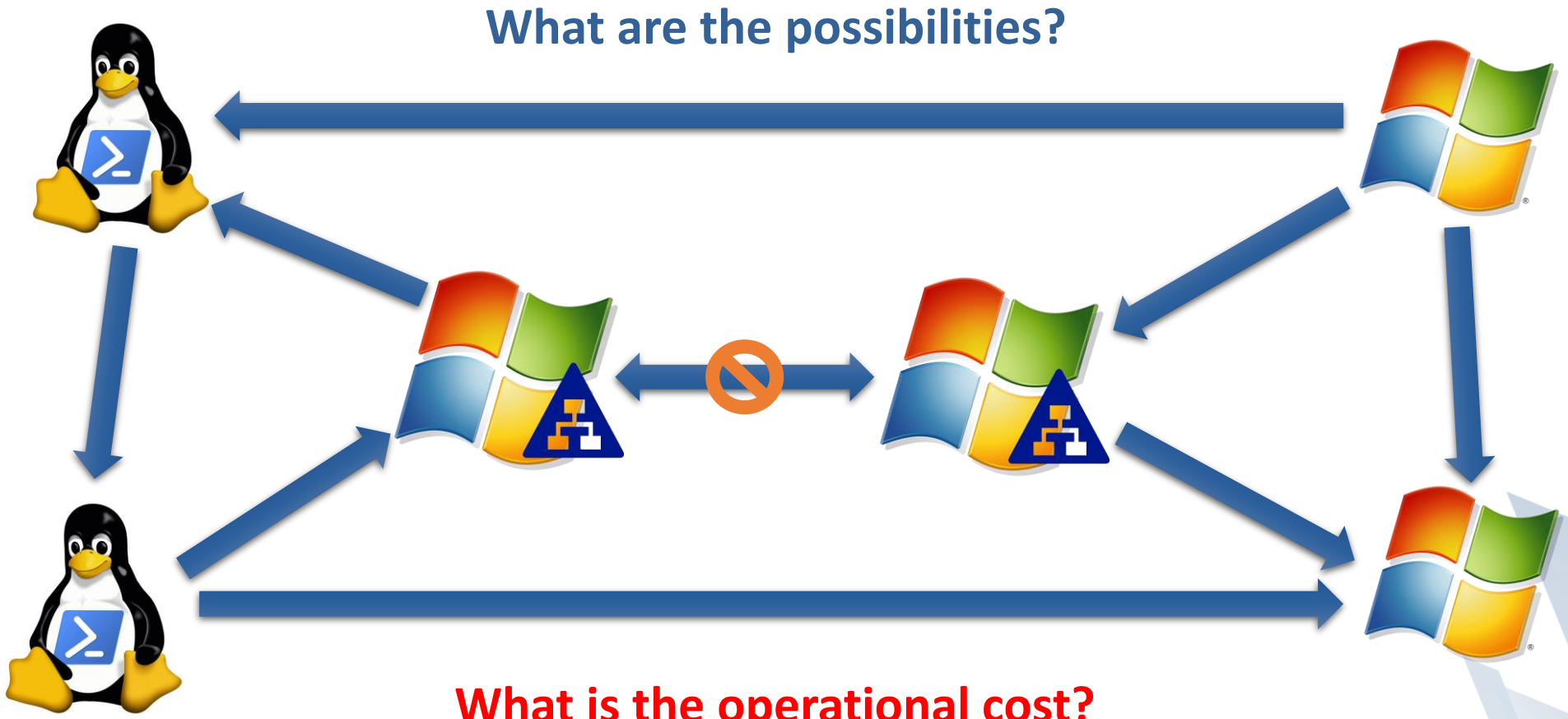
- installing additional components
  - as opposed to: using existing ones
- changing target machine(s) configurations
  - probably at scale – HOW?
  - opening standard protocols reduces security posture
- changing source machine(s) configurations
- as little additional preparation work as possible

Applied Connectology

Who is talking to whom, how and what about

@cj_berlin

Connectology 101



@cj_berlin

WinRM without Kerberos

- HTTPS with cleartext creds
  - Target must be configured to listen on HTTPS and to present a certificate
  - Source must be configured to trust that certificate (chain)
- TrustedHosts + Fresh credentials delegation
  - Source must be configured to trust Target
  - Source must be configured to delegate credentials
  - Trusted Hosts * → giving creds to malicious hosts!

Let‘s talk about SSH remoting

PSCONF.EU Antwerp24

PowerShell

Copy

```
Enter-PSSession
      [-HostName] <String>
      [-Options <Hashtable>]
      [-Port <Int32>]
      [-UserName <String>]
      [-KeyFilePath <String>]
      [-Subsystem <String>]
      [-ConnectingTimeout <Int32>]
      [-SSHTransport]
      [<CommonParameters>]
```

- UserName can be **DOM\user** or **user@linuxhost**
- No way to specify Password or SecurePassword
- Zero touch connection requires a key file from user (domain/target)
  - …but without password to protect it!
  - Correct permissions on key files!

Demo

SSH to Windows

SSH to Linux

PSCONF.EU

Antwerp 24

@cj_berlin

WinRM vs. SSH smackdown

	WinRM	SSH
PowerShell requirements	Windows to Windows only Win PowerShell 3+ or PowerShell	Windows or Linux PowerShell
Preparation	TrustedHosts + delegation **on Source** **or** WinRM/HTTPS **on Target** Cert Trust **on Source**	Enable pwsh subsystem in SSH **on Target** *(sshd installed as part of OS)*
Permissions on Target	Admin or Remote Management	-
JEA	Yes	No
Zero touch requirements	Knowledge of credentials	Key file prepared on target

Beyond PSRemoting

Sometimes a step back opens a way forward

@cj_berlin

Using SSH for… SSH

- **PoSh-SSH** by Carlos Perez wraps *Renci SSHNet*
  - beautifully, at that <3
- New-SSHSession + Invoke-SSHCommand
  - Be mindful of timeouts with long-running commands!
- For sudo on Linux:

```
' echo "{0}"|sudo -s {1}' -f $password, $command
```

  - May not work on every Linux distro, depending on **sudo**
- also great for: SCP, Command Streams etc.

WMI ~~and~~ or CIM

- Use CIM cmdlets, they said. It is the future, they said.
- CIM uses WinRM by default → same as PSRemoting
  - Fallback to WMI: `New-CIMSessionOption -Protocol DCOM`
  - DCOM sessions are faster than WMI. Much faster.

Demo

WMI and CIM

PSCONF.EU

Antwerp 24

@cj_berlin

Demo

WMI shenanigans

PSCONF.EU

Antwerp 24

@cj_berlin

What else is there?

- So many remote services can run executables locally…
- More often than not even in a privileged context…

Demo

Remoting Hacks

PSCONF.EU

Antwerp 24

@cj_berlin

Q&A

15 minutes

@cj_berlin