PSDAY.UK

2019

The current state of PowerShell remoting

Christian Lehrer

IRONGATE WEALTH MANAGEMENT

ScriptRunner®
Make PowerShell a real solution

PSDAY.UK

2019

About_me

Name: Christian Lehrer

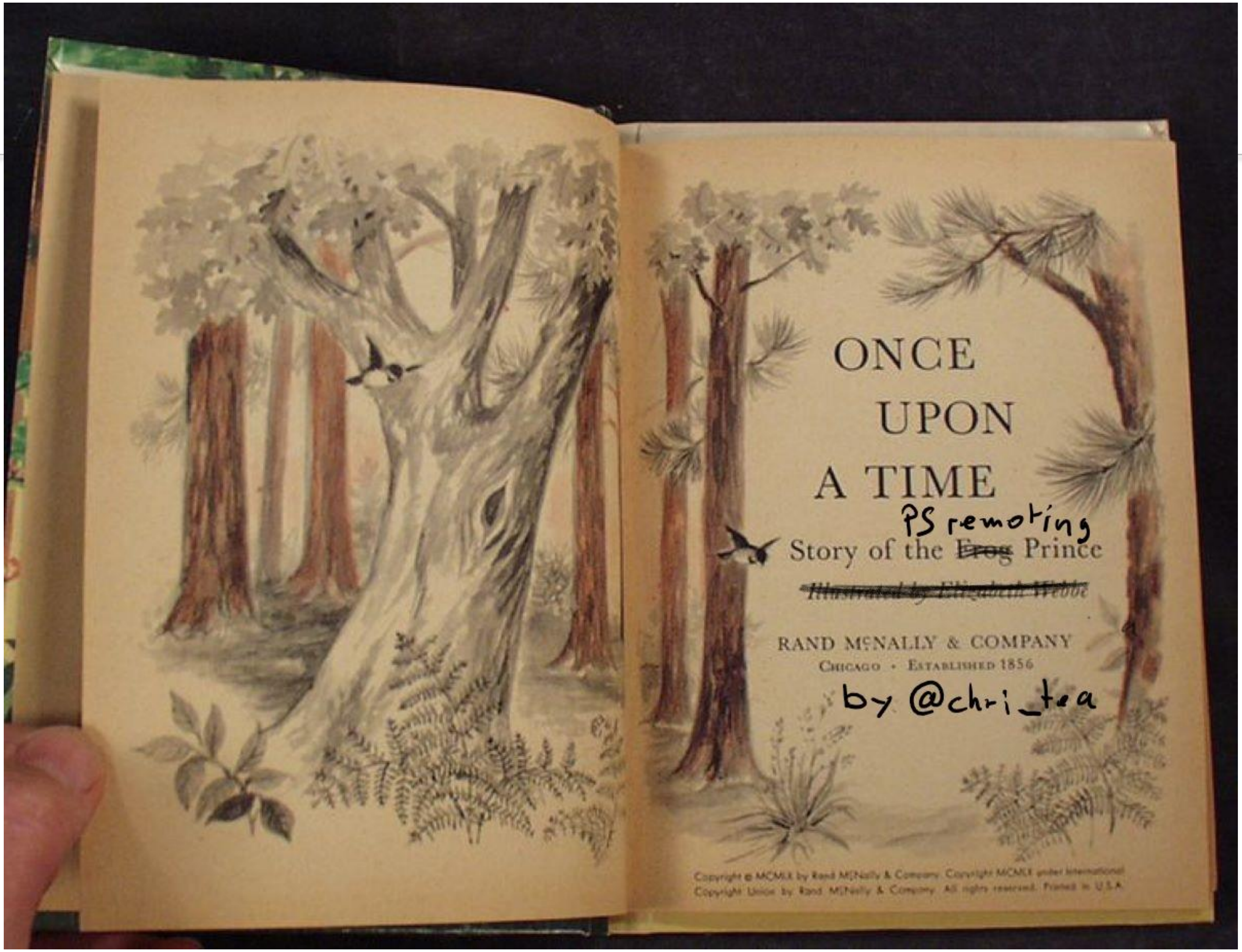
twitter: @chri_tea

works at: sepago®

The current state of PowerShell remoting

A tail of a man who tried to get PowerShell remoting running (cross-platform)

- A beginning of a tail as it should be
- The technical story within the tail (Or: the 2 1/2 possible transport layers usable for PowerShell remoting and how they differ)
- Peak tragedy (Or: Christian vs. PSRP)
- Not all hope is lost (Or: Christian + openSSH)
- And he PSremoted even after (Or: some tipps on how to get you PS remoting a little contained)



ONCE UPON A TIME

Story of the ~~Frog~~ PS remoting Prince

~~Illustrated by Elizabeth Webbe~~

RAND McNALLY & COMPANY
CHICAGO · ESTABLISHED 1856

by @chri_tea

PowerShell remoting transport protocols

WindowsRemoteManagement / WebServices for Management / PowerShellRemotingProtocol

The Web Services for Management (WS-Management) Specification describes a Web services 291 protocol based on SOAP for use in management-specific domains. These domains include […]PCs, servers, devices, Web services and other applications, and other 293 manageable entities. (from the standards description).

WinRM implements the WSMan protocol for use in Windows.

PSRP enhances the limitations of pure WinRM (especially possible packet size) and makes full PowerShell remoting available.

Benefits:

- in the box since Windows Vista
- easy configuration
- secure transport and authentication (when unchanged)
- JEACustom configurations

Drawbacks:

- only fully functional on Windows
- by default only administrators can connect via PS-remoting (can be changed)

PowerShell remoting transport protocols

SecureSHell / PowerShellRemotingProtocol

SSH is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command line, login, and remote command execution, but any network service can be secured with SSH. (Wikipedia)

Benefits:

- Well known (since Windows 10 1709/Server 2016 also natively in Windows through OpenSSH)
- secure authentication
- even non-admins can use PS-remoting (without admin-permission)

Drawbacks:

- No JEA
- no custom configurations
- no support on older Windows versions

Wsman in a multi-OS world

Setting up on Windows with Windows PowerShell

Windows Vista and above

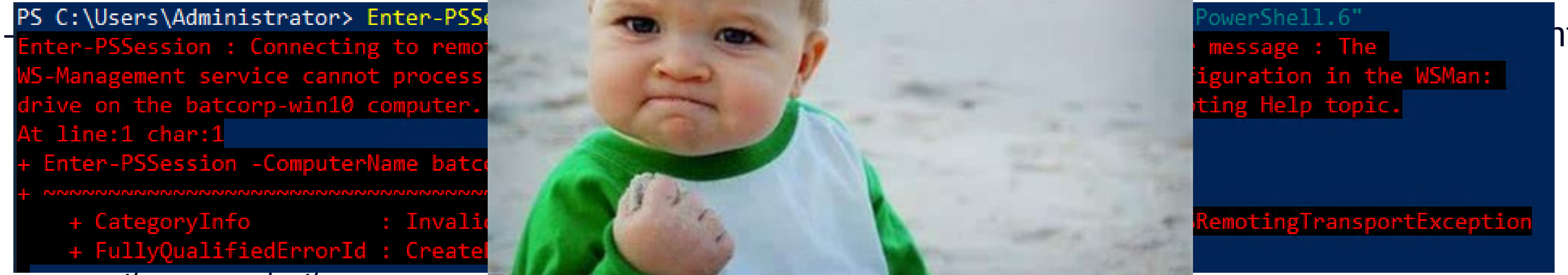
- ≥ Installation:
  - – No installation needed.
- ≥ Configuration
  - – Check the running state of the WinRM service
  - – WinRm quickconfig (sets-up default configuration for the WSMan listener)
  - – Allow traffic (port 5985, 5986)through the firewall

- Since Windows Server2012 WSMan is set up with the default configuration out of the box. This allows PS remoting access from private or domain networks for members of the administrators group.
- DEMO

Wsman in a multi-OS world

Setting up on Windows with PowerShell Core for Windows

- Installation:
  - No installation needed.
- Configuration
  - nt be



```
PS C:\Users\Administrator> Enter-PSSe                                   PowerShell.6"
Enter-PSSession : Connecting to remo                                  message : The
WS-Management service cannot process                                  iguration in the WSMan:
drive on the batcorp-win10 computer.                                  ting Help topic.
At line:1 char:1
+ Enter-PSSession -ComputerName batc
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : Invali                                  RemotingTransportException
    + FullyQualifiedErrorId : Create
```

  - WinRm must be running
  - Allow traffic (port 5985, 5986)through the firewall
- DEMO PS5.1 to PSCore6.2

2019

Wsman

Setting up

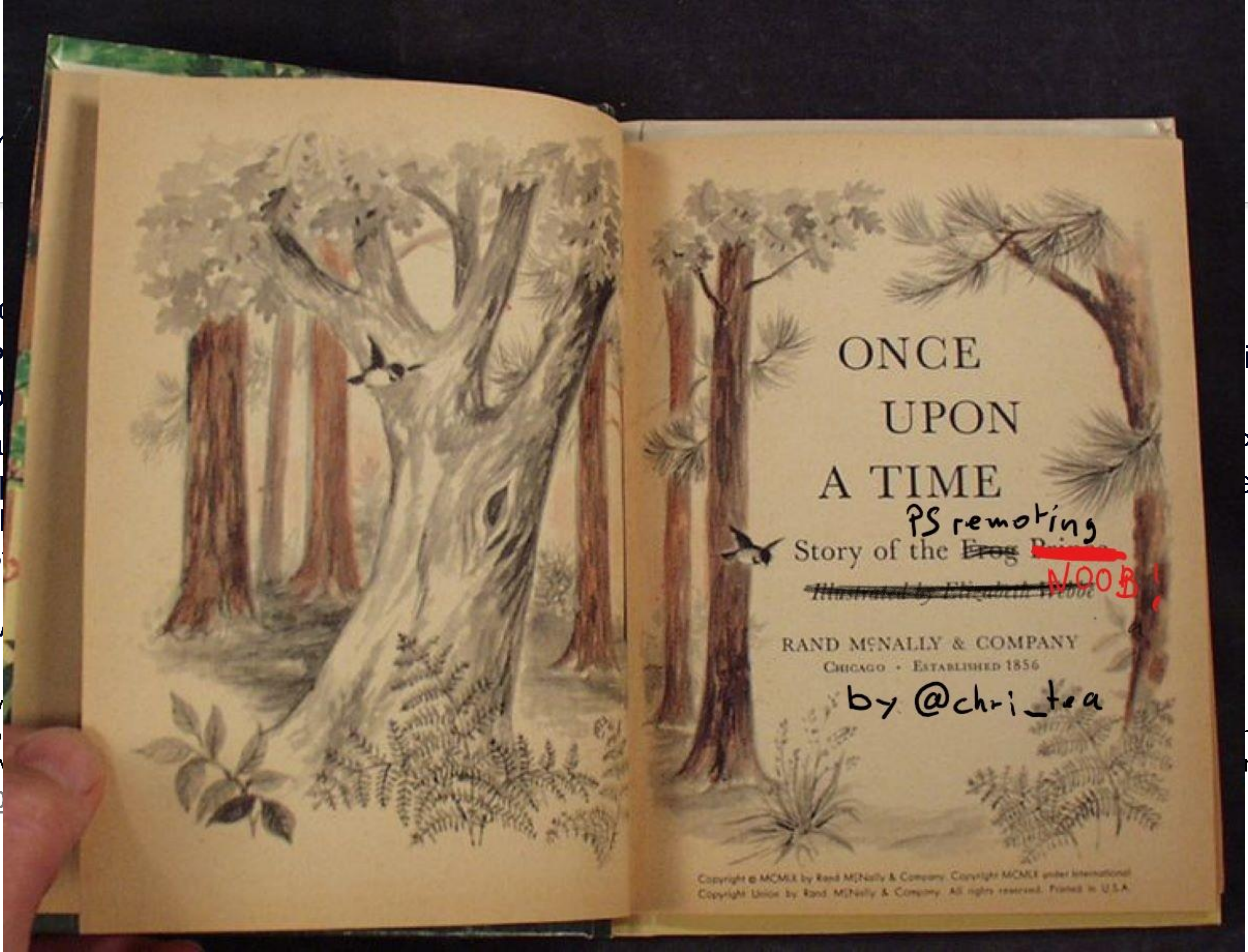
≥ Installati

– PSRP is
OMI p

• Sta part
(lib erver
PSI
pro

Nev

“Pow
prob his is
to inv red.“
http



ONCE
UPON
A TIME
PS remoting
Story of the ~~Frog Prince~~ NOOB!
~~Illustrated by Elizabeth Webbe~~

RAND McNALLY & COMPANY
Chicago · Established 1856

by @chri_tea

Copyright © MCMLX by Rand McNally & Company. Copyright MCMLX under International
Copyright Union by Rand McNally & Company. All rights reserved. Printed in U.S.A.

2019

Wsman in a multi-OS world

Setting up on MacOS with P

Shit, no macbook. -> Presenta

Wsman in a multi-OS world

Setting up on MacOS with PowerShell Core

≥ Installation:
  - OpenSSL -> was already on box
  - Basic auth -> not supported by PowerShell Core
  - SPNEGO -> not supported by Apple

  - Christian: ¯_(ツ)_/¯

Trying it with OpenSSH

Setting up OpenSSH on Windows 10 1709 or Server 2016 and above

- ≥ Get-WindowsCapability -Online | where {$_.name -like "openssh.server*"} | Add-WindowsCapability –Online
- ≥ Get-WindowsCapability -Online | where {$_.name -like "openssh.client*"} | Add-WindowsCapability –Online
- ≥ (get-service *ssh* | Set-Service -StartupType manual) (or automatic for constant use)
- ≥ Start services (get-service *ssh* | Start-Service)

Trying it with OpenSSH

Setting up OpenSSH on Windows 10 1709 or Server 2016 and above

≥ Change sshd_config ($env:ProgramData\ssh) to allow password authentication and add in the PWSH subsystem:

- PasswordAuthentication yes
- Subsystem   powershell c:/program files/powershell/6/pwsh.exe -sshs -NoLogo –NoProfile
  - Corrected: Subsystem   powershell c:/pwsh/pwsh.exe -sshs -NoLogo –NoProfile

  (after creating symbolic link with new-item -ItemType SymbolicLink -path c:\ -name "pwsh" -Value "C:\Program Files\PowerShell\6\„)
- Restart services
- Check if openSSH installation created the correct firewall rule (Port22 TCP)

DEMO

Trying with openSSH

Setting SSH for PS remoting on Ubuntu 18.04

≥ Installation:
  - Install openSSH server and client if not already on the box (sudo apt install openssh-server/client)
  - Configure sshd.config

    PasswordAuthentication yes

    Subsystem powershell %yourpathtopwsh% -sshs –noLogo –noProfile
  - Restart service

Trying with openSSH

Setting SSH for PS remoting on MacOS

- Installation:
  - openSSH should be on the box already, if not check brew to install it
  - Enable remote management (System preferences, sharing, remote login on, select users to access)
  - Configure sshd.config (private/etc/ssh/sshd_config)

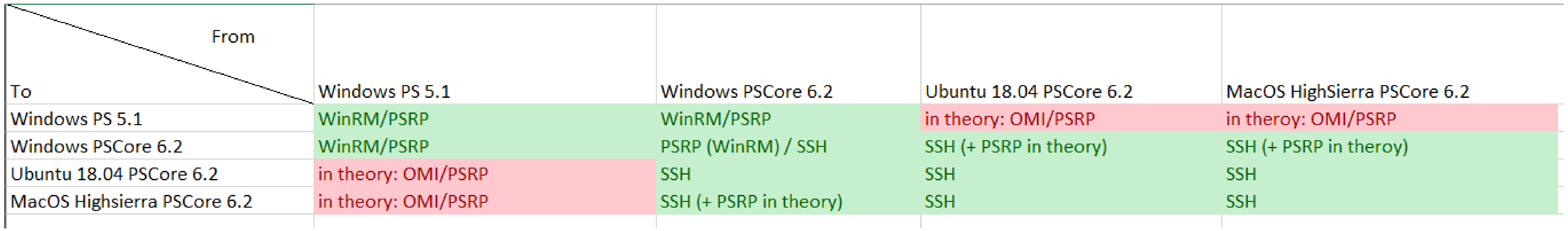
    PasswordAuthentication yes

    Subsystem powershell /usr/local/bin/pwsh -sshs –noLogo –noProfile
  - Restart service (sudo launchctl stop com.openssh.sshd, sudo launchctl start com.openssh.sshd)

- DEMO (W10->MacOS)
- DEMO (U1804->MacOS)
- DEMO (MacOS->Linux)

2019

Overview



From To	Windows PS 5.1	Windows PSCore 6.2	Ubuntu 18.04 PSCore 6.2	MacOS HighSierra PSCore 6.2
Windows PS 5.1	WinRM/PSRP	WinRM/PSRP	in theory: OMI/PSRP	in theroy: OMI/PSRP
Windows PSCore 6.2	WinRM/PSRP	PSRP (WinRM) / SSH	SSH (+ PSRP in theory)	SSH (+ PSRP in theroy)
Ubuntu 18.04 PSCore 6.2	in theory: OMI/PSRP	SSH	SSH	SSH
MacOS Highsierra PSCore 6.2	in theory: OMI/PSRP	SSH (+ PSRP in theory)	SSH	SSH

Comment from Richard Siddaway: In non-domain joined Windows scenarios, go for SSH also!

Making use of the openSSH possibilities

Private / Public key authentication

≥ On windows host:
  - Configure sshd_conf
    - comment out #AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
  - Restart sshd service
  - Install module “OpenSSHUtils”

Making use of the openSSH possibilities

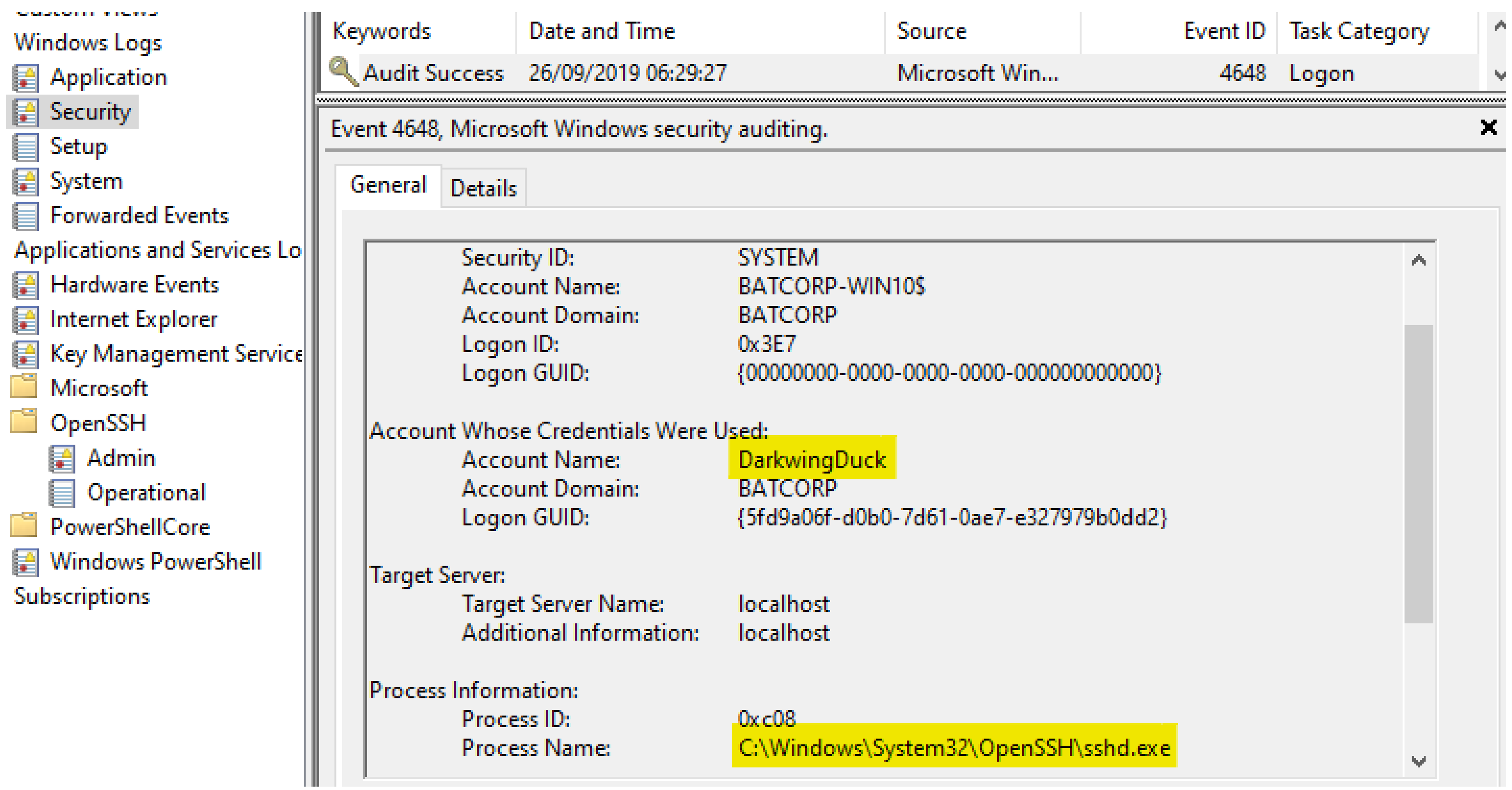
Private / Public key authentication

≥ On MacOS/Linux Client:
  – Create a public / private key pair
  – Upload the public part to the .ssh folder of the windows users you want to be logged in as
  – Repair permissions with „repair-authorizedkeys“ from openSSHUtils module (be careful!)

≥ DEMO

≥ DEMO

Detecting SSH logins on Windows



```
Windows Logs
  Application
  Security
  Setup
  System
  Forwarded Events
Applications and Services Lo
  Hardware Events
  Internet Explorer
  Key Management Service
  Microsoft
  OpenSSH
    Admin
    Operational
  PowerShellCore
  Windows PowerShell
Subscriptions
```

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	26/09/2019 06:29:27	Microsoft Win...	4648	Logon

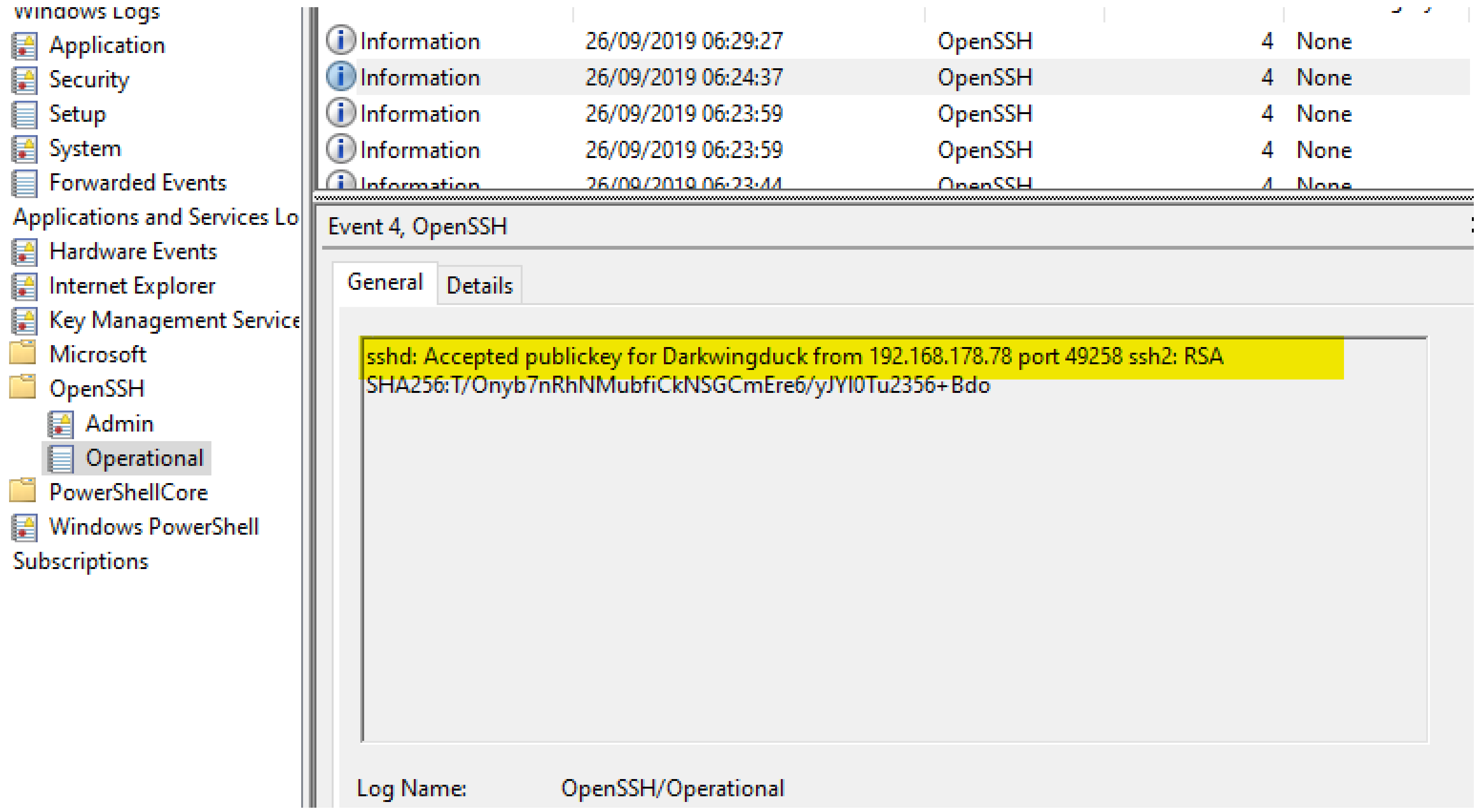
Event 4648, Microsoft Windows security auditing.

General | Details

```
        Security ID:                SYSTEM
        Account Name:               BATCORP-WIN10$
        Account Domain:             BATCORP
        Logon ID:                   0x3E7
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:               DarkwingDuck
        Account Domain:             BATCORP
        Logon GUID:                 {5fd9a06f-d0b0-7d61-0ae7-e327979b0dd2}

Target Server:
        Target Server Name:         localhost
        Additional Information:     localhost

Process Information:
        Process ID:                 0xc08
        Process Name:               C:\Windows\System32\OpenSSH\sshd.exe
```

2019

Detecting SSH logins on Windows



Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Hardware Events
Internet Explorer
Key Management Service
Microsoft
OpenSSH
Admin
Operational
PowerShellCore
Windows PowerShell
Subscriptions

```
Information   26/09/2019 06:29:27   OpenSSH   4   None
Information   26/09/2019 06:24:37   OpenSSH   4   None
Information   26/09/2019 06:23:59   OpenSSH   4   None
Information   26/09/2019 06:23:59   OpenSSH   4   None
Information   26/09/2019 06:23:44   OpenSSH   4   None
```

Event 4, OpenSSH

General | Details

```
sshd: Accepted publickey for Darkwingduck from 192.168.178.78 port 49258 ssh2: RSA
SHA256:T/Onyb7nRhNMubfiCkNSGCmEre6/yJYI0Tu2356+Bdo
```

Log Name: OpenSSH/Operational

Contain the use of PS Remoting

JEA

~~WSMan configuration (Filters)~~ -> Possible, but don´t

Firewall-rules

sshd config

PSDAY.UK

2019

PSDAY.UK

2019

PSDAY.UK
2019

Thank you

IRONGATE
WEALTH MANAGEMENT

ScriptRunner®
Make PowerShell a real solution

PSDAY.UK

2019