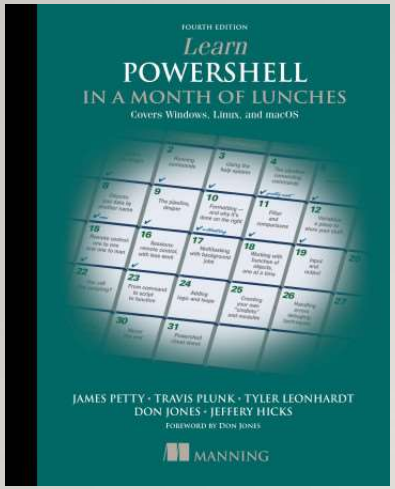
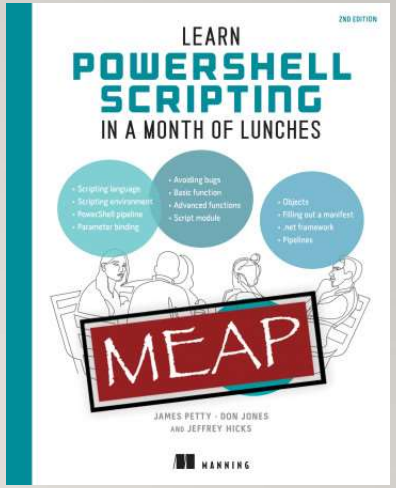
POWERSHELL SECURITY AND BEST PRACTICES



JAMES PETTY

@psjamesp
Github.com/psjamesp

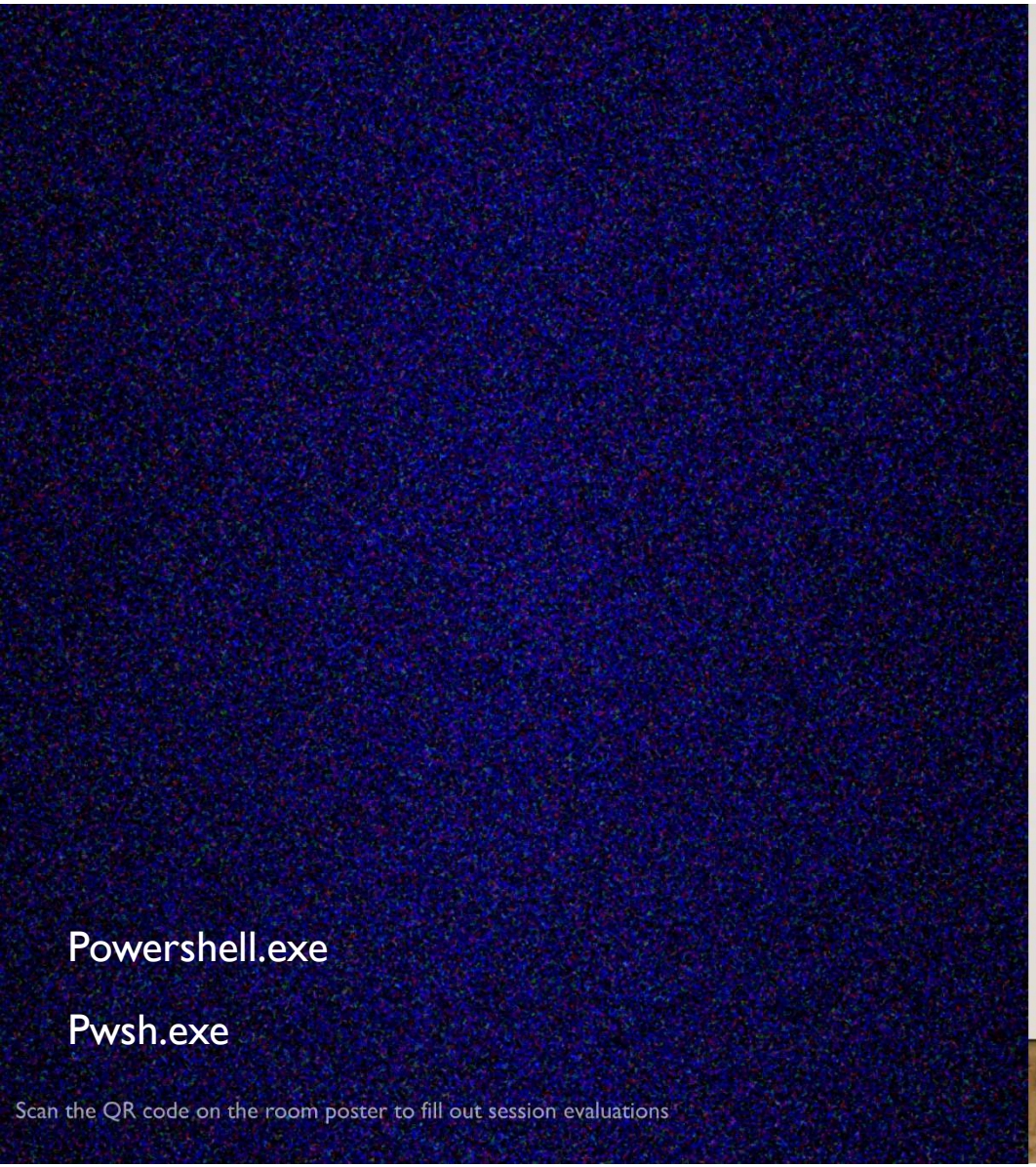


MVP Microsoft® Most Valuable Professional

HTTPS://GITHUB.COM/PSJAMESP/PRESENTATIONS

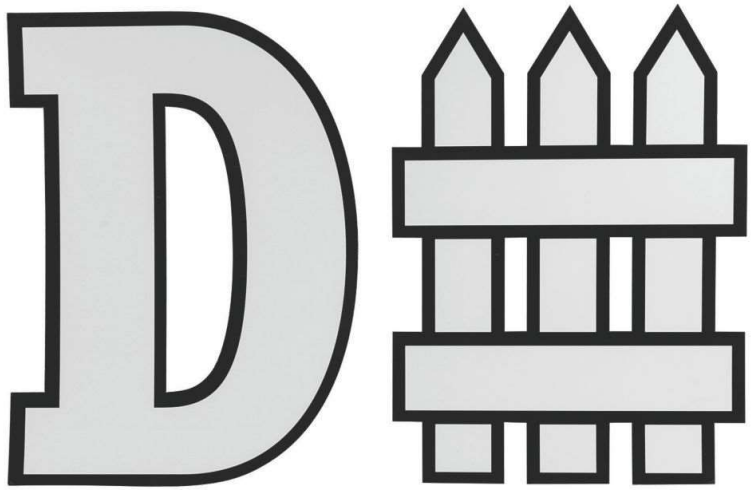
POWERSHELL

Windows PowerShell	PowerShell
5.1 – last release	7.4 – Latest
.Net	.Net Core



POWERSHELL IS NOT A VIRUS

There are numerous virus that use PowerShell as the launch pad for their attack



Scan the QR code on the room poster to fill out session evaluations

SECURITY POLICY

- AllSigned
- Bypass
- Default
- RemoteSigned
- Restricted
- Undefined
- Unrestricted

Scan the QR code on the room poster to fill out session evaluations

SECURITY POLICY SCOPES

- MachinePolicy
- UserPolicy
- Process
- CurrentUser
- LocalMachine

POWERSHELL REMOTING

Windows PowerShell

- WinRM
  - Port 5985 (HTTP)
  - Port 5986 (HTTPS)

PowerShell

- WinRM
  - Port 5985 (HTTP)
  - Port 5986 (HTTPS)
- SSH
  - Port 22

REMOTING WITHPOWERSHELL

SSH	WinRM
-HostName	-ComputerName

Thank you.