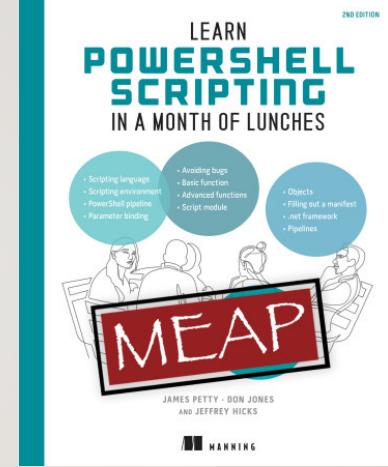
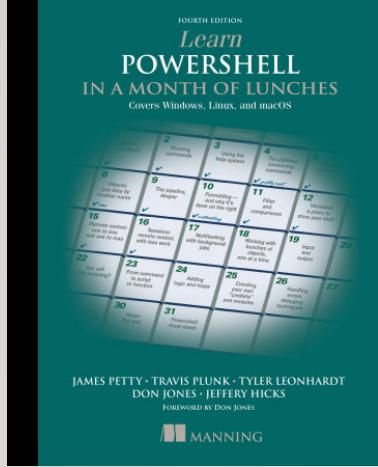


POWERSHELL SECURITY AND BEST PRACTICES





JAMES PETTY

@psjamesp
[Github.com/psjamesp](https://github.com/psjamesp)



POWERSHELL

Windows PowerShell

5.1 – last release

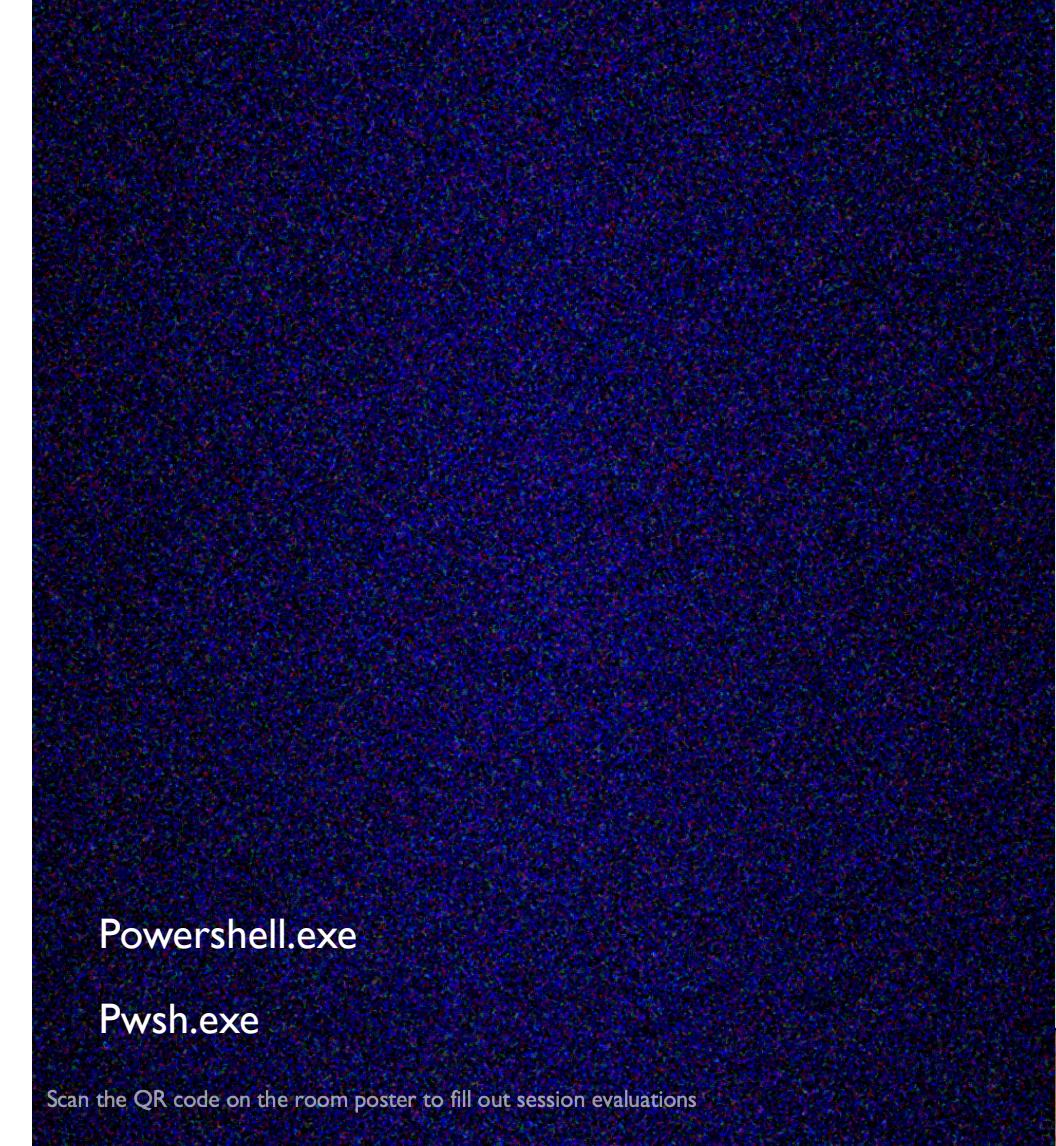
.Net

PowerShell

7.3.6 – Latest

.Net Core





**POWERSHELL
IS NOT A
VIRUS**

Powershell.exe

Pwsh.exe

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



WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

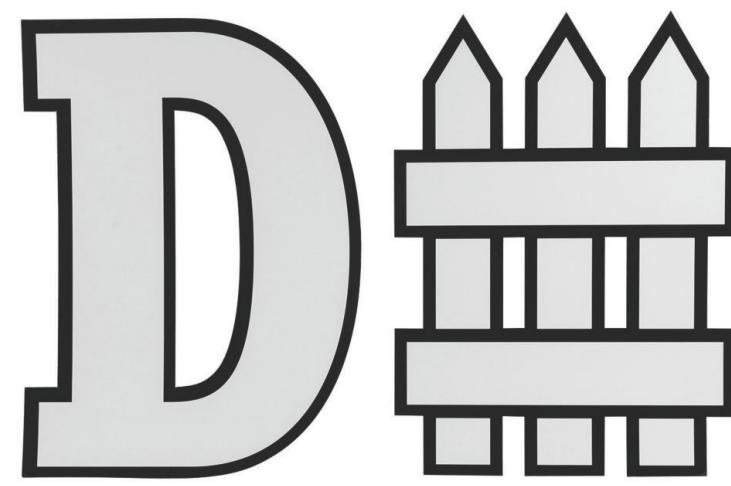
(High Priority Virus Removal Call Line)

Your IP Address: [REDACTED] | Generated on [REDACTED] | Priority: Urgent



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

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

AllSigned

Bypass

Default

RemoteSigned

Restricted

Undefined

Unrestricted

SECURITY POLICY SCOPES

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

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 WITH POWERSHELL

SSH

-HostName

WinRM

-ComputerName



Thank you.

