SECURE360

Why Learn PowerShell?

Examples of Awesome

Presented by:
Derek Ardolf

SECURE360

About The Speaker

- Derek Ardolf
- Systems Development Engineer
- Certified VE PowerShell Toolmaker
- Taught PowerShell at Century College

- Twitter: @ScriptAutomate
- GitHub: ScriptAutomate

SECURE360

Agenda

- PowerShell?
- RDP vs. PSRemoting
- Examples of Easy Wins
- Resources

SECURE360

Quick! Do an Audit

- Just received an email from InfoSec Team
- Must audit local administrators group on targeted sample of machines in domain
- Process requires screenshots to be placed in a Word document...

DEPRESSING DEMO

Moral of The Story

#DevSecOps or #DevDerpOps
What will you embrace?

SECURE360

PowerShell?

- Created by Jeffrey Snover, Technical Fellow @ Microsoft
- First released in 2006: Brand new, decade-old tech
- Exists by default in every Windows system, starting with Server 2008 R2
- Internally, all teams at Microsoft are required to provide (at a minimum) the same functionality in PowerShell that you can do in the GUI

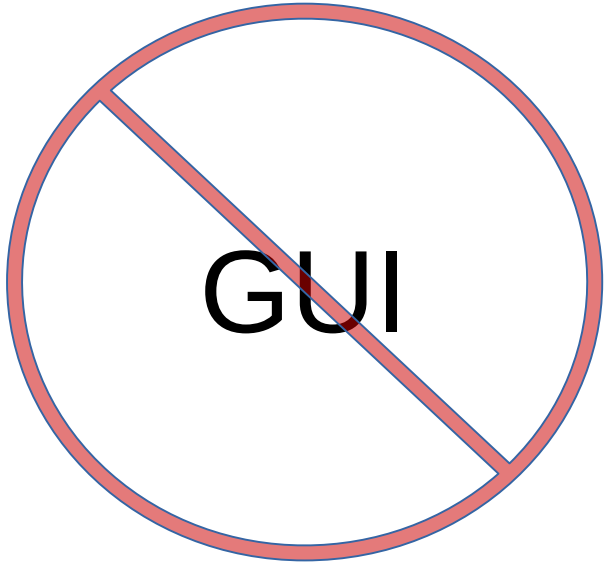
PowerShell? Cont.

- Server Core: Default OS install, no GUI
- Nano Server: No GUI, no 32-bit libraries, no GPOs
  - Size: Base server is 410MB
  - Reduced Patching: 1/10th the number of critical patches
  - Less rebooting: ~75% less patches requiring reboots
  - Minimum required open ports: Reduced from 34 to 12
- Deprecation and Replacement
  - AD Users and Computers (ADUC) → AD Administrative Center (ADAC)
  - Group Policy For Servers → Desired State Configuration (DSC)

SECURE360

RDP vs. PSRemoting

- *"GUIs are like heroin – it's amazing at first...but before you know it, you're dying in an alley."* Jeffrey Snover



GUI

Server

Desktop / Client

SECURE360

RDP vs. PSRemoting

- PowerShell Remoting
  - Single port (5985 TCP default / 5986 TCP for SSL)
  - No more LSASS sass
  - No GUI/RDP needed
  - Automate all the things
  - Traffic is encrypted by default
    - Can use SSL / certificates
  - Version 5: Awesome Auditing and Just Enough Admin (JEA)

Examples of Easy Wins

- Active Directory Group Audits
  - DEMO
    - RSAT Tools
    - GitHub Gist of Demo Code

Examples of Easy Wins Cont.

- Group Managed Service Accounts
  - Passwordless service accounts?!
  - Can only create and register with PowerShell
  - Drop ADUC. Pick up ADAC!
    - ADAC has a cool PowerShell History tab/log
  - DEMO
    - GitHub Gist of Demo Code

SECURE360

Examples of Easy Wins Cont.

- Miscellaneous
  - PowerShell can be used to query:
    - Internal websites
    - CMDBs
    - Databases
    - REST APIs
- JSON representation of policy means portability
- PowerShell is only one example of awesome
  - Other scripting languages like Python, Ruby, etc. can only help, too, as they are cross-platform and work on Linux

SECURE360

Resources

- The Monad Manifesto: The original Snover-authored doc that led to PowerShell
- MVA: all free courses matching PowerShell (from introductory to advanced)
- The Scripting Guy Blog
- PowerShell Team Blog
- PowerShell.org / DevOps Collective
- Open Sourced PowerShell.Org eBooks (free to download, optional pay) [GitHub Source]
- PowerShell + DevOps Summit and Misc Videos YouTube Channel
- PowerShell WMF v4 and WMF v5 Download Landing Pages
- PowerShell Cheat Sheet Downloads
- Remote System Administration Tools (RSAT) Downloads and Directions
- Jeffrey Snover Presentation on Just Enough Admin (JEA)
- JEA Step by Step Landing Page and White Paper (and GitHub repo)
- PowerShell Team GitHub / PowerShell.org GitHub
- Code used in this presentation [GitHub Gist]
- My GitHub Profile / Repositories, including AuditTools Module from demo