TECHMENTOR CONFERENCES

ORLANDO 2010

WINDOWS SERVERS SECURITY VIRTUALIZATION MICROSOFT R2 TECHNOLOGY POWERSHELL SHAREPOINT

Top 10 Command Line Tools You MUST Know

Jeffery Hicks

The Lonely Administrator

Pre-requisites for this presentation:

1) Basic Windows Administration
2) Some CLI Experience

Level: Intermediate

What's this all about?

- Old School is back in style
- GUI's have limits
- No scripting, but scriptable
- 10 favorite CLI based tools
- Demos available from my blog

CLI Tips

- Run elevated
- Get help with /? Or -?
- Yahbinoogle is your friend
- Do I really have to remind you to test in a non-production environment?

1. CACLS/(XCACLS)/ICACLS

- Work with File and Folder permissions
- Different flavors depending on need and OS
- The best way to manage bulk permission changes

```
C:\> icacls %userprofile%
```

2. SUBINACL (RK Tool)

- The Swiss Army Knife of security
- Free download from Microsoft
- Not for the squeamish

```
C:\> subinacl /help /full
```

3. REG.EXE

- Command line registry management
- Works locally and remotely
- Only HKLM and HKU remotely

```
C:\> REG QUERY
"HKLM\Software\Microsoft\windows
NT\currentversion" /v RegisteredOwner
```

4. SCHTASKS.EXE

- OS Specific versions
- Manage tasks locally and remotely
- Query/Run/Create/Delete

```
C:\> schtasks /query /s Server01
```

5. NETDOM.EXE

- Manage a computer's network identity
- Features vary by OS
- Works locally and remotely

```
C:\>netdom query /domain:mycompany
/userd:mycompany\administrator
/passwordd:* FSMP
```

6. TaskList & TaskKill

- CLI version of task manager
- Works locally and remotely
- Show all tasks or filter

```
C:\>tasklist /s SRV02 /fi "ImageName eq
foo.exe"
C:\>taskkill /s SRV02 /im notepad.exe
```

7. NET

- NET User
- NET localgroup
- NET View
- NET Time

- `C:\> net localgroup Administrators`

8. Robocopy

- The definitive CLI copy tool
- Great for backup and synchronization
- Many, many options

```
C:\> robocopy c:\files x:\backup /s /xf
*.tmp /eta
```

9. NETSH.EXE

- The best CLI networking tool
- Use interactively or as a command
- Uses “contexts”
- Show or Dump configurations

```
C:\>netsh dnsclient show state
```

10. SC.EXE

- CLI Service Management
- Query one service or many
- Works locally and remotely

```
C:\>sc \\SRV01 query spooler
```

Extra Credit (Win7)

- SUBST.EXE
- NETSTAT.EXE
- WHOAMI.EXE
- SYSTEMINFO.EXE
- DNSCMD.EXE
- QUSER.EXE

What's in your toolbox?

Questions

Enjoy The Show

http://jdhitsolutions.com/blog