Hey, Scripting Guy! Blog

Learn about Windows PowerShell

The 2011 Scripting Games Advanced Event 1: Finding Process Module Versions by Using PowerShell

ScriptingGuy1 4 Apr 2011 1:15 AM 6

Summary: Advanced Event 1 of the 2011 Scripting games entails using Windows PowerShell to find process module versions.

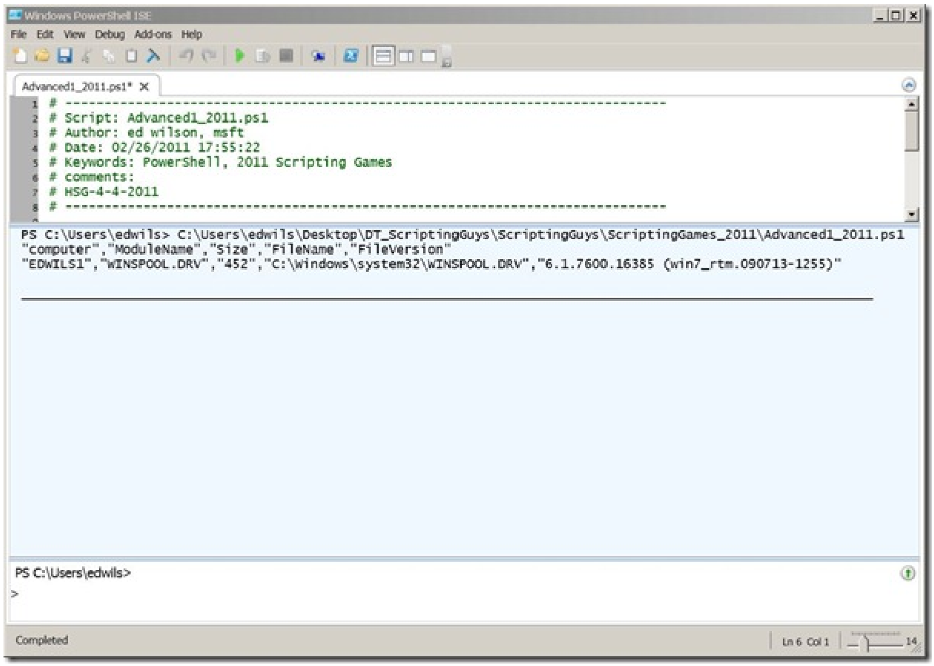
About this event

Division	Advanced
Date of Event	4/4/2011 12:15 AM
Due Date	4/11/2011 12:15 AM

Event scenario

You are the network administrator for a small business with 200 users and four servers on the network. You are responsible for managing Active Directory Domain Services (AD DS) running on a single Windows Server 2008 R2 machine, Exchange Server 2007 running on Windows Server 2008, SQL Server 2008 also running on a Windows Server 2008 machine, and a File and Print Server running Windows Server 2003. Your workstations are a combination of Windows XP, Windows Vista and Windows 7. Because one of your servers also runs Windows Software Update Services (WSUS), you have deployed Windows PowerShell 2.0 to all of your workstations and servers on the network. Your boss, who is the CIO and the comptroller was listening to the radio on the way into work today, and he heard a report about a zero-day exploit of a particular component. The radio report mentioned the name of the component, and it stated that it only existed on certain servers. Unfortunately, the reporter was a bit vague with the details. Because of this vagueness, your boss wants you to scan every machine on the network for the affected component.

For the purposes of this event, you will only need to run the script against your local computer, but you should include the capability to run it against multiple machines. You should use the Notepad process, and report the version of the *"Windows Spooler Driver"* module that is used by the Notepad process. You should display a Comma Separated Value output with a header and values for the following: ModuleName, Size, FileName, FileVersion. A sample output is shown in the following image.



```
# -----------------------------------------------------------------------------
# Script: Advanced1_2011.ps1
# Author: ed wilson, msft
# Date: 02/26/2011 17:55:22
# Keywords: PowerShell, 2011 Scripting Games
# comments:
# HSG-4-4-2011
# -----------------------------------------------------------------------------
```

```
PS C:\Users\edwils> C:\Users\edwils\Desktop\DT_ScriptingGuys\ScriptingGuys\ScriptingGames_2011\Advanced1_2011.ps1
"computer","ModuleName","Size","FileName","FileVersion"
"EDWILS1","WINSPOOL.DRV","452","C:\Windows\system32\WINSPOOL.DRV","6.1.7600.16385 (win7_rtm.090713-1255)"
```

```
PS C:\Users\edwils>
>
```

Design points

- Your code should be completely reusable
- If the methodology you use to retrieve the information does not provide its own remoting mechanism, you should incorporate code to utilize Windows PowerShell remoting
- You do not need to output to a CSV file, but your output should be in such a format that redirection arrows (>>) would produce a CSV file
- Extra points for accepting command-line arguments
- Extra points for writing an advanced function that is suitable to incorporate into a module
- Extra points if your script reads AD DS to retrieve the list of computers to query

2011 Scripting Games links

2011 Scripting Games: All Links on One Page

Submit your scripts on PoshCode

Support our Sponsors!

I invite you to follow me on Twitter and Facebook. If you have any questions, send email to me at scripter@microsoft.com, or post your questions on the Official Scripting Guys Forum. Good luck as you compete in this year's Scripting Games. We wish you well.

Ed Wilson, Microsoft Scripting Guy

Tweet 31 Share 20 Save this on Delicious

Comments

5 Apr 2011 9:42 AM

Zak

Hi,

are we to asume that PSremoting is enabled on all of the servers?

Tnx

6 Apr 2011 2:06 AM

jmc1029

Are we assuming that notepad is already running on the systems or (as Zak mentioned) PSremoting is enabled?

6 Apr 2011 2:30 AM

Justin

+1 to Zak and jmc1029 . Both drastically change the script parameters.

IamMred 6 Apr 2011 3:30 PM

@zak yes you can assume that PSRemoting is enabled on all the servers. You will gain extra points if you include the ability to test to see if remoting is enabled and operating correctly. In addition, logging is always a good thing (i.e. write to a log that says attempt to connect failed and log the reason). You might also want to check for rights to perform PowerShell remoting.

@jmc1029 Yes you can assume notepad is already running. But you should handle the exception that arises when attempting to get information on a non-existant process. If you then start the process / get the information and / stop the process you will get a better score.

@Justin For all (10 Advanced Events) you should write robust code and do everything you can think of to ensure you script will run in an enterprise environment. My suggestions for additional points are that ... simply suggestions. Depending on the approach you take, my suggestions will either become essential or completely irrelevant. That is why I wrote the guidelines a bit vague (in most cases).

hassan sayed issa20014 4 Aug 2014 9:02 PM

thank you

hassan sayed issa20014 4 Aug 2014 9:02 PM

thank you