6-2 Activity: Scripting Administrative Tasks

Joshua Merren

Southern New Hampshire University
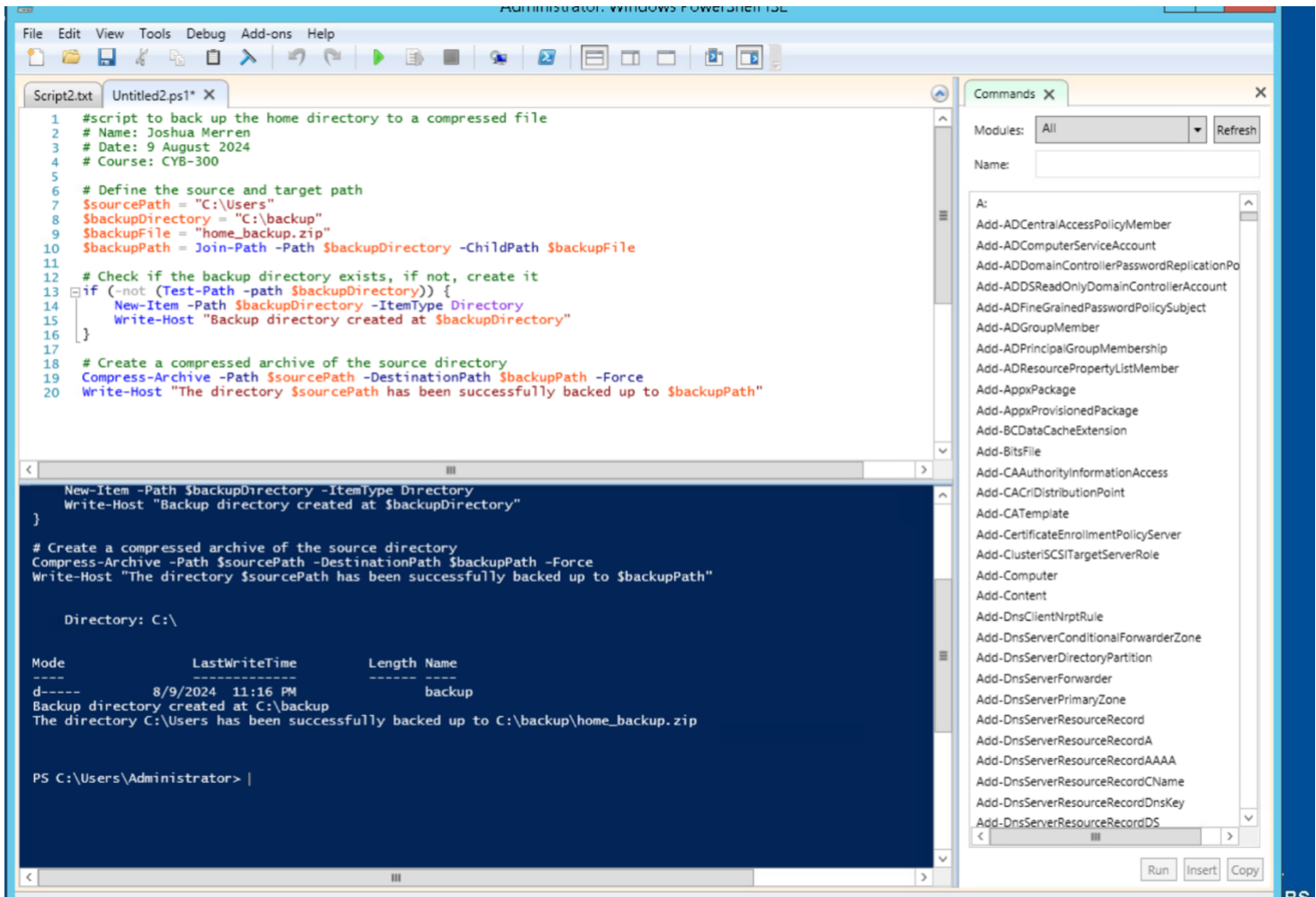
CYB-300-11432-M01 System and Comm Security

Professor Robert Chubbuck

9 August 2024

Script 1 screenshots

Script to back up the home directory to a compressed file

Script 2 Screenshots

Script to retrieve and save a list of all running processes

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1* X

```
1   #script to list all running processes and output to a text file
2   # Name: Joshua Merren
3   # Date: 9 August 2024
4   # Course: CYB-300
5
6   Import-Module ActiveDirectory
7
8   # Define the path to the output file on the Desktop
9   $desktopPath = [Environment]::GetFolderPath("Desktop")
10  $outputFile = "running_processes.txt"
11  $outputPath = Join-Path -Path $desktopPath -ChildPath $outputFile
12
13  # Retrieve all currently running processes
14  $processes = Get-Process
15
16  # Output the processes to the specified text file
17  $processes | Out-File -FilePath $outputPath
18
19  # Confirm completion in the console
20  Write-Host "A list of all running processes has been saved to $outputPath"
```

```
PS C:\Users\Administrator> #script to list all running processes and output to a text file
# Name: Joshua Merren
# Date: 9 August 2024
# Course: CYB-300

Import-Module ActiveDirectory

# Define the path to the output file on the Desktop
$desktopPath = [Environment]::GetFolderPath("Desktop")
$outputFile = "running_processes.txt"
$outputPath = Join-Path -Path $desktopPath -ChildPath $outputFile

# Retrieve all currently running processes
$processes = Get-Process

# Output the processes to the specified text file
$processes | Out-File -FilePath $outputPath

# Confirm completion in the console
Write-Host "A list of all running processes has been saved to $outputPath"
A list of all running processes has been saved to C:\Users\Administrator\Desktop\running_processes.txt

PS C:\Users\Administrator>
```

Commands X

Modules: All   Refresh

Name:

A:
Add-ADCentralAccessPolicyMember
Add-ADComputerServiceAccount
Add-ADDomainControllerPasswordReplicationPo
Add-ADDSReadOnlyDomainControllerAccount
Add-ADFineGrainedPasswordPolicySubject
Add-ADGroupMember
Add-ADPrincipalGroupMembership
Add-ADResourcePropertyListMember
Add-AppxPackage
Add-AppxProvisionedPackage
Add-BCDataCacheExtension
Add-BitsFile
Add-CAAuthorityInformationAccess
Add-CACriDistributionPoint
Add-CATemplate
Add-CertificateEnrollmentPolicyServer
Add-ClusteriSCSITargetServerRole
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DnsServerConditionalForwarderZone
Add-DnsServerDirectoryPartition
Add-DnsServerForwarder
Add-DnsServerPrimaryZone
Add-DnsServerResourceRecord
Add-DnsServerResourceRecordA
Add-DnsServerResourceRecordAAAA

Run Insert Copy

Completed   Ln 20 Col 75   100%

running_processes - Notepad

File Edit Format View Help

```
Handles  NPM(K)    PM(K)    WS(K)    CPU(s)    Id  SI ProcessName
-------  ------    -----    -----    ------    --  -- -----------
    367      30    11532    15776     0.06   1344   0 certsrv
    228      12     1600     3628     0.09    304   0 csrss
    151      12     1652    15544     0.13    408   1 csrss
    328      31    13852    18268     0.09   1400   0 dfsrs
    123      11     1724     5148     0.00   1924   0 dfssvc
    191      13     3152     9984     0.03   2564   0 dllhost
  10276   10214    90508    88164     0.34   1480   0 dns
    176      19    26740    43844     0.09    816   1 dwm
   1229      57    45836    88504     6.61   3280   1 explorer
      0       0        0        4                0   0 Idle
    143      14     5952    12152     0.03   1500   0 inetinfo
     89      11     1396     4276     0.02   1540   0 ismserv
   1533     176    56064    58212     1.53    500   0 lsass
    343      42    50160    61952     0.78   1292   0 Microsoft.ActiveDirectory.WebServices
    151      12     2376     6688     0.03   2964   0 msdtc
    124       8     1220     4912     0.02   1612   0 ocspsvc
    637      68   140852   175552     9.98   3220   1 powershell_ise
    441      45   100336    54452     1.52   3680   1 ServerManager
    289      11     3644     7840     0.38    492   0 services
     52       2      268     1020     0.06    200   0 smss
    369      20     3052     8808     0.06   1260   0 spoolsv
    361      33    10632    12576     0.16    288   0 svchost
    371      15     3336     9904     0.09    644   0 svchost
    374      18     2988     7120     0.14    688   0 svchost
    450      18    14088    17048     0.47    804   0 svchost
   1365      50    17084    33284     1.38    856   0 svchost
    753      26     6100    12048     0.13    916   0 svchost
    563      34     6724    15132     0.13    984   0 svchost
    111      11     3204     7392     0.05   1328   0 svchost
    158      14     3996     8032     0.06   1880   0 svchost
    388      18     3252     7660     0.00   2460   0 svchost
    240      19     8096    10664     0.06   2500   0 svchost
    105       8     1448     4500     0.00   2548   0 svchost
```

PLABDC01
(none)
Administrator
PRACTICELABS