

Lab10-PowershellScripting

Ben W

SYS255

FA23

Deliverables:

1. Command alias: grep = Select-String

```
Administrator: Windows PowerShell
PS C:\Users\ben-adm\scripting> cat .\text.txt
Here are some words
This is some other words
Here is the word test
I am going to "grep" this file
more words on the end here
PS C:\Users\ben-adm\scripting> grep
grep : The term 'grep' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of
the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ grep
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (grep:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\ben-adm\scripting> Set-Alias -Name grep -Value Select-String
PS C:\Users\ben-adm\scripting> grep

cmdlet Select-String at command pipeline position 1
Supply values for the following parameters:
Pattern[0]: test
Pattern[1]:
Path[0]: text.txt
Path[1]:

text.txt:3:Here is the word test

PS C:\Users\ben-adm\scripting> grep -Pattern test -Path .\text.txt

text.txt:3:Here is the word test

PS C:\Users\ben-adm\scripting> _
```

2. Servers.ps1 script

```
Administrator: Windows PowerShell
PS C:\Users\ben-adm\scripting> cat .\servers.ps1
$servers = cat .\servers.txt
foreach($server in $servers) {
    echo "Pinging $server"
    ping -n 1 $server
}
PS C:\Users\ben-adm\scripting> .\servers.ps1
Pinging champlain.edu
Pinging champlain.edu [208.115.107.132] with 32 bytes of data:
Reply from 208.115.107.132: bytes=32 time=73ms TTL=48

Ping statistics for 208.115.107.132:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 73ms, Maximum = 73ms, Average = 73ms
Pinging vermont.gov
Pinging vermont.gov [199.107.32.183] with 32 bytes of data:
Reply from 199.107.32.183: bytes=32 time=24ms TTL=237

Ping statistics for 199.107.32.183:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 24ms, Average = 24ms
Pinging mcsp.one
Pinging mcsp.one [217.160.0.8] with 32 bytes of data:
Reply from 217.160.0.8: bytes=32 time=107ms TTL=51

Ping statistics for 217.160.0.8:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 107ms, Maximum = 107ms, Average = 107ms
PS C:\Users\ben-adm\scripting> █
```

3. Resolve Script

```
Administrator: Windows PowerShell
PS C:\Users\ben-adm\scripting> cat .\resolve.ps1
param([string] $type, [string] $server)

$servers = cat $server

foreach($serv in $servers) {
    Resolve-DnsName $serv -Type $type | Select-Object Name, IPAddress
}
PS C:\Users\ben-adm\scripting> .\resolve.ps1 -type A -server .\servers.txt

Name                IPAddress
----                -
champlain.edu       208.115.107.132
vermont.gov         199.107.32.183
mcsp.one            217.160.0.8

PS C:\Users\ben-adm\scripting> █
```

4. Remote PS Session

```
PS C:\Users\ben-adm\scripting> Get-ADComputer -Filter * | Select-Object Name
Name
----
AD02-BENJAMIN
WKS02-BENJAMIN
FS01-BENJAMIN
WEB01-BENJAMIN
BLOG01-BENJAMIN

PS C:\Users\ben-adm\scripting> Enter-PSSession -ComputerName FS01-BENJAMIN
[FS01-BENJAMIN]: PS C:\Users\ben-adm\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9db8:5de3:2a02:b978%6
    IPv4 Address. . . . . : 10.0.5.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.5.2
[FS01-BENJAMIN]: PS C:\Users\ben-adm\Documents> █
```

5. Remote PS Command

```
PS C:\Users\ben-adm\scripting> Invoke-Command -ComputerName FS01-BENJAMIN -ScriptBlock { ping -n 1 localhost }

Pinging fs01-benjamin.ben.local [::1] with 32 bytes of data:
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\ben-adm\scripting>
```

6. AD Management

```
PS C:\Users\ben-adm\scripting> New-ADUser -Name "Joe"
PS C:\Users\ben-adm\scripting> New-ADGroup -Name "Nerds" -GroupCategory Security -GroupScope DomainLocal
PS C:\Users\ben-adm\scripting> Add-ADGroupMember -Identity Nerds -Members Joe
PS C:\Users\ben-adm\scripting> Get-ADGroupMember -Identity Nerds

distinguishedName : CN=Joe,CN=Users,DC=ben,DC=local
name               : Joe
objectClass        : user
objectGUID         : b5b439ea-3913-4a98-aaba-43377983a32d
SamAccountName     : Joe
SID                : S-1-5-21-3046433430-1214274579-1171965080-1112
```

7. Remote command on workstation

```
PS C:\Users\ben-adm\scripting> Invoke-Command -ComputerName WKS02-BENJAMIN -ScriptBlock {ipconfig}

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : ben.local
    IPv4 Address. . . . . : 10.0.5.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.5.2
PS C:\Users\ben-adm\scripting>
```