```
  Id CommandLine
  -- -----------
   1 cd\
   2 cls
   3 Get-Command -verb get -noun *event*
   4 cls
   5 Get-Command -verb get -noun *event*
   6 help Get-EventLog
   7 Get-EventLog -List
   8 help Get-EventLog -Parameter computername
   9 help Get-EventLog -ShowWindow
  10 cls
  11 Get-EventLog -LogName System -Newest 1
  12 Get-EventLog -LogName System -Newest 1 | Get-Member
  13 Get-EventLog -LogName System -Newest 1 | Get-Member -MemberType
Property
  14 Get-EventLog -LogName System -Newest 1 | Get-Member -MemberType
Properties
  15 Get-EventLog -LogName System -Newest 1 | Format-List *
  16 Get-EventLog -LogName System -Newest 1
  17 Get-EventLog -LogName System -Newest 1 | select time
  18 Get-EventLog -LogName System -Newest 1 | select TimeGenerated
  19 Get-EventLog -LogName System -Newest 1 | select TimeGenerated,
EntryTyp...
  20 Get-EventLog -LogName System -EntryType Error -Newest 1 | select
```

```
TimeGe...
  21 Get-EventLog -LogName System -EntryType Error -Newest 1 | select
TimeGe...
  22 cls

  23 Get-EventLog -LogName System -Newest 1

  24 Start-Job {Get-EventLog -ComputerName sql02, web02 -LogName System
-New...
  25 Get-Job

  26 Invoke-Command -ComputerName dc02, sql02, web02 {Get-NetFirewallRule
-D...
  27 Invoke-Command -ComputerName dc02, sql02, web02 {Get-NetFirewallRule
-D...
  28 get-job

  29 get-job | Receive-Job -Keep

  30 get-job | Remove-Job

  31 get-job

  32 $error[0]

  33 $error

  34 gcm Get-NetFirewallRule

  35 Get-Command -Module NetSecurity

  36 Get-Command Get-NetFirewallRule | fl *

  37 cls

  38 Get-Command Get-NetFirewallRule | select Definition

  39 Get-Command Get-NetFirewallRule | select -expand Definition

  40 (Get-Command Get-NetFirewallRule).Definition

  41 (Get-Command Get-NetFirewallRule) | gm -MemberType Property

  42 Start-Job {Get-EventLog -ComputerName sql02, web02 -LogName System
```

```
-New...
  43 Get-Job

  44 Get-Job | Receive-Job -Keep

  45 Get-Job

  46 $a = Get-Job | Receive-Job

  47 Get-Job

  48 Get-Job | Receive-Job

  49 Get-Job | Receive-Job -AutoRemoveJob

  50 Get-Job | Receive-Job -AutoRemoveJob -Wait

  51 $a

  52 $a | Format-List *

  53 $a | Get-Member

  54 cls

  55 Get-EventLog -LogName System -Message '*join*domain*failed*'

  56 Get-EventLog -LogName System -InstanceId 4097

  57 Get-EventLog -LogName System -Index 639

  58 Get-EventLog -LogName System | Group-Object Message | select -First 10

  59 Get-EventLog -LogName System | Group-Object Message -NoElement |
select...
  60 Get-EventLog -LogName System | Group-Object Message -NoElement |
select...
  61 Get-EventLog -LogName System | Group-Object Message -NoElement | sort
-...
  62 cls

  63 help Get-WinEvent

  64 Get-WinEvent -ListLog *
```

```
  65 (Get-WinEvent -ListLog *).count

  66 Get-WinEvent -ListLog | where recordcount

  67 Get-WinEvent -ListLog * | where recordcount

  68 Get-WinEvent -ListLog * | where recordcount -gt 10

  69 Get-WinEvent -ListLog * | where recordcount -gt 100

  70 Show-EventLog

  71 cls

  72 $xml = @'...

  73 cls

  74 $xml

  75 Get-WinEvent -FilterXml $xml

  76 Get-WinEvent -FilterXPath "*[System[(Level=2) and (EventID=4097) and
Ti...
  77 Get-WinEvent -LogName system  -FilterXPath "*[System[(Level=2) and
(Eve...
  78 Get-WinEvent -LogName system  -FilterXPath "*[System[(Level=2) and
(Eve...
  79 Get-WinEvent -LogName system  -FilterXPath "*[System[EventID=4097 and
T...
  80 Get-WinEvent -LogName system  -FilterXPath "*[system[EventID=4097 and
T...
  81 Get-WinEvent -LogName system  -FilterXPath "*[System[EventID=4097 and
T...
  82 Get-WinEvent -LogName system  -FilterXPath "*[System[EventID=4097]]"

  83 Get-WinEvent -LogName system  -FilterXPath "*[System[EventID=4097]]" |
...
  84 Get-WinEvent -LogName system  -FilterXPath "*[System[EventID=4097]]" |
...
  85 Stop-Service bits | gm

  86 Stop-Service bits
```

```
  87 Stop-Service bits -PassThru | gm

  88 cls

  89 Get-WinEvent -FilterHashtable @{LogName='System';ID=4097}

  90 Get-WinEvent -FilterHashtable
@{LogName='System';ID=4097;StartTime=(Get...
  91 help Get-WinEvent

  92 Get-WinEvent -ListProvider 'Microsoft-Windows-Kernel-General'

  93 Get-WinEvent -ProviderName 'Microsoft-Windows-PowerShell' -MaxEvents 1

  94 Get-WinEvent -ProviderName 'Microsoft-Windows-PowerShell' -MaxEvents 1
...
  95 Get-WinEvent -ProviderName 'Microsoft-Windows-PowerShell' -MaxEvents 1
...
  96 Get-WmiObject -Class Win32_ntlog* -List

  97 Get-WmiObject -Class Win32_ntlogevent -filter {Logfile='System' and
Eve...
  98 Get-WmiObject -Class Win32_nteventlogfile -filter {Logfile='System'}

  99 Get-WmiObject -Class Win32_nteventlog* -List

 100 Get-WmiObject -Class Win32_nteventlogfile

 101 Get-WmiObject -Class Win32_nteventlogfile {LogFileName='System'}

 102 Get-WmiObject -Class Win32_nteventlogfile -Filter
{LogFileName='System'}
 103 Get-WmiObject -Class Win32_nteventlogfile -Filter
{LogFileName='System'...
 104 (Get-WmiObject -Class Win32_nteventlogfile -Filter
{LogFileName='System...
 105 (Get-WmiObject -Class Win32_nteventlogfile -Filter
{LogFileName='System...
 106 Get-WinEvent -Path C:\tmp\systemlog.evtx -FilterXPath
"*[System[EventID...
 107 cls

 108 help Get-History
```

```
 109 Get-WmiObject -Class Win32_ntlog* -List

 110 Get-CimInstance -ClassName win32_nteventlogfile

 111 Get-CimInstance -ClassName win32_nteventlogfile -Filter
{LogFileName='S...
 112 Get-CimInstance -ClassName win32_nteventlogfile -Filter
"LogFileName='S...
 113 cls

 114 [System.Diagnostics.EventLog]::GetEventLogs()

 115 [System.Diagnostics.EventLog]::GetEventLogs('dc01')

 116 [System.Diagnostics.EventLog]::GetEventLogs()[5]

 117 [System.Diagnostics.EventLog]::GetEventLogs()[5].Entries | where
eventi...
 118 [System.Diagnostics.EventLog]::Exists("System")

 119 [System.Diagnostics.EventLog]::Exists("12345")

 120
[System.Diagnostics.EventLog]::LogNameFromSourceName("Microsoft-Windows...
 121
[System.Diagnostics.EventLog]::LogNameFromSourceName("Microsoft-Windows...
 122 Get-WinEvent -ListProvider 'Microsoft-Windows-Kernal-General'

 123 Get-WinEvent -ListProvider 'Microsoft-Windows-Kernel-General'

 124 help about_eventlogs

 125 help about

 126 'Chad,Josh,Michael,Robert' -split ',' | Get-Random -Count 2

 127 write-host "Michael & Josh send contact info to mspsug@gmail.com"
```