



CYBER RANGERS
ARMORING YOUR BUSINESS



POWERSHELL BASIC SCRIPTING

MODULE 1: POWERSHELL INTRODUCTION

Jan Marek | Cyber Rangers

CEH | CHFI | CompTIA Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Ethical Hacker, Forensic Investigator & Security Engineer

jan@cyber-rangers.com | www.cyber-rangers.com



AGENDA

- What is PowerShell
- How to run PowerShell on Windows, Linux and MacOS
- How to find needed commands and help for these commands
- Some examples of very useful cmdlets
- Console and Script Editors
- PowerShell Profile



WHAT IS POWERSHELL

- Scripting engine and scripting language
- Windows integrated
- Application integrated
- Cloud integrated
- Automation and administration



HOW TO RUN POWERSHELL ON WINDOWS, LINUX AND MACOS

- Windows
 - Windows PowerShell [built-in]: powershell.exe
 - PowerShell (6) Core [installation required]: pwsh.exe
 - PowerShell 7 [installation required]: pwsh.exe
- Linux
 - PowerShell 7 [installation required]: pwsh
- MacOS
 - PowerShell 7 [installation required]: pwsh



COMMANDS, CMDLETS, PARAMETERS

- Cmdlet vs. command vs. function vs. ...
- Parameters
 - Positional
 - Named
 - Required
 - Optional



HOW TO FIND NEEDED COMMANDS AND GET HELP

- <http://docs.microsoft.com>

Get-Command

Get-Command -Name *service*

Get-Command -Verb get

Update-Help

Update-Help -Module dism

Save-Help -Module dism -DestinationPath C:\temp

Update-Help -SourcePath C:\temp

Get-Help

Get-Help -Name Get-Service

Get-Help -Name Get-Process -Online

Get-Help About_Pester



ALIAS

Get-Alias

Get-Alias -Definition Get-ChildItem

New-Alias -Name psdir -value Get-ChildItem



SOME EXAMPLES OF VERY USEFUL CMDLETS

▪ # Verb-Noun

Out-File

Get-Service

Get-Process

Get-EventLog

Get-WinEvent -LogName Application -MaxEvents 10

Get-Volume

Get-Disk

Get-ADUser -Filter *

Set-Service -Name Spooler -StartupType Automatic

Get-Certificate

Get-DnsClientCache

Get-NetRoute

Get-NetIPAddress

New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.1 -PrefixLength 24 -DefaultGateway 10.0.0.254

And so and so...



CONSOLE AND SCRIPT EDITORS (1/3)

The image shows two overlapping windows from Windows PowerShell ISE. The background window is titled 'Windows PowerShell ISE' and displays a script file named 'mod001-002.ps1'. The script contains the following commands:

```
1 # Verb-Noun
2
3 Get-Service
4 Get-Process
5 Get-EventLog
6 Get-WinEvent -LogName Application -MaxEvents 10
7 Get-Volume
8 Get-Disk
9 Get-ADUser -Filter *
```

The foreground window is titled 'Administrator: Windows PowerShell' and shows the execution of the command `$env:COMPUTERNAME`, which returns the output `DESKTOP-L6HDDCD`. The prompt is `PS C:\Users\JanMarek>`.

At the bottom of the PowerShell ISE window, the status bar shows 'Completed', 'Ln 1 Col 23', and a zoom level of '115%'.



CONSOLE AND SCRIPT EDITORS (2/3)

```
C:\Windows\system32\cmd.exe - powershell

(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\JanMarek>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\JanMarek> $env:USERNAME
JanMarek
PS C:\Users\JanMarek>
```

```
Windows PowerShell x PowerShell 7 x + v - □ x

PS C:\Users\JanMarek> $env:USERPROFILE
C:\Users\JanMarek
PS C:\Users\JanMarek>
```

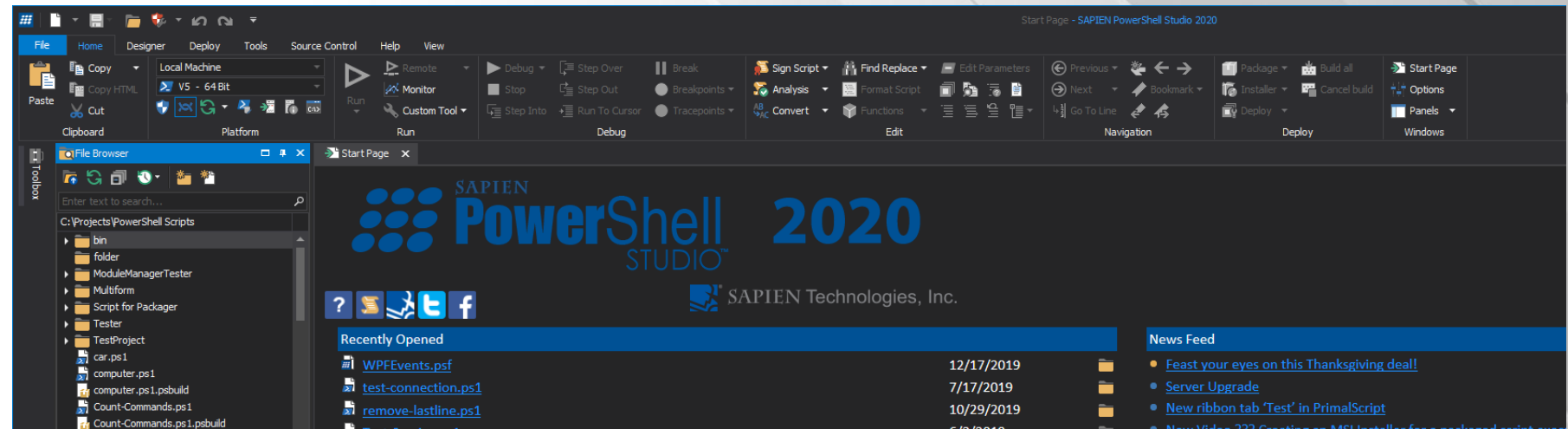


CONSOLE AND SCRIPT EDITORS (3/3)

The screenshot shows the Visual Studio Code interface. The top menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. The main editor window displays a file named 'test.ps1' with the following content:

```
> test.ps1  
C: > Users > JanMarek > OneDrive - Cyber Rangers > Desktop > > test.ps1  
1 # this is the best!
```

Below the editor, the 'TERMINAL' tab is active, showing a PowerShell prompt: 'PS C:\Users\JanMarek>'. The status bar at the bottom indicates 'Ln 1, Col 11', 'Spaces: 4', 'UTF-8', 'CRLF', 'PowerShell', and '7.0'.





POWERSHELL PROFILE

```
Administrator: Windows PowerShell
PS C:\Windows\system32> $profile
C:\Users\JanMarek\OneDrive - Cyber Rangers\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1
PS C:\Windows\system32> '$env:username' | Out-File $profile
PS C:\Windows\system32>
```

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled3.ps1* X
1 $profile
2 '$env:computername' | Out-File $profile
PS C:\Users\JanMarek> $profile
'$env:computername' | Out-File $profile
C:\Users\JanMarek\OneDrive - Cyber Rangers\Documents\WindowsPowerShell\Microsoft.PowerShellISE_profile.ps1
PS C:\Users\JanMarek>
Completed | Ln 5 Col 23 | 115%
```



POWERSHELL 7 PROFILE

```
PowerShell 7 x + v  
PS C:\Users\JanMarek> $profile  
C:\Users\JanMarek\OneDrive - Cyber Rangers\Documents\PowerShell\Microsoft.PowerShell_profile.ps1  
  
PS C:\Users\JanMarek>
```

```
File Edit Selection View Go Run Terminal Help • test.ps1 - Visual Studio Code  
test.ps1  
C: > Users > JanMarek > OneDrive - Cyber Rangers > Desktop > test.ps1  
1 $profile  
  
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: PowerShell Integrated Console v2020.6.0  
===== PowerShell Integrated Console v2020.6.0 =====  
PS C:\Users\JanMarek> $profile  
C:\Users\JanMarek\OneDrive - Cyber Rangers\Documents\PowerShell\Microsoft.VSCode_profile.ps1  
PS C:\Users\JanMarek>  
  
Ln 1, Col 9 Spaces: 4 UTF-8 CRLF PowerShell 7.0
```



POWERSHELL 101

- Strings (single quotes vs double quotes)

- 'text'
- "text"

- Escape character

```
Get-Command `
    -Verb Get `
    -Noun Service
```

- Comments

```
#this is comment
```

```
<# this is block  
comment  
#>
```

- Tab key, shorten parameters

```
Get-Command -na get-help
```



LAB

- ✦ Find commands
- ✦ Find help
- ✦ Use found commands
- ✦ Create your own PowerShell profile



POWERSHELL BASIC SCRIPTING

MODULE 1: POWERSHELL INTRODUCTION

Jan Marek | Cyber Rangers

CEH | CHFI | CompTIA Pentest+ | CEI | MVP | MCT | MCC | MCSA | MCSE

Ethical Hacker, Forensic Investigator & Security Engineer

jan@cyber-rangers.com | www.cyber-rangers.com



CYBER RANGERS
ARMORING YOUR BUSINESS