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
```

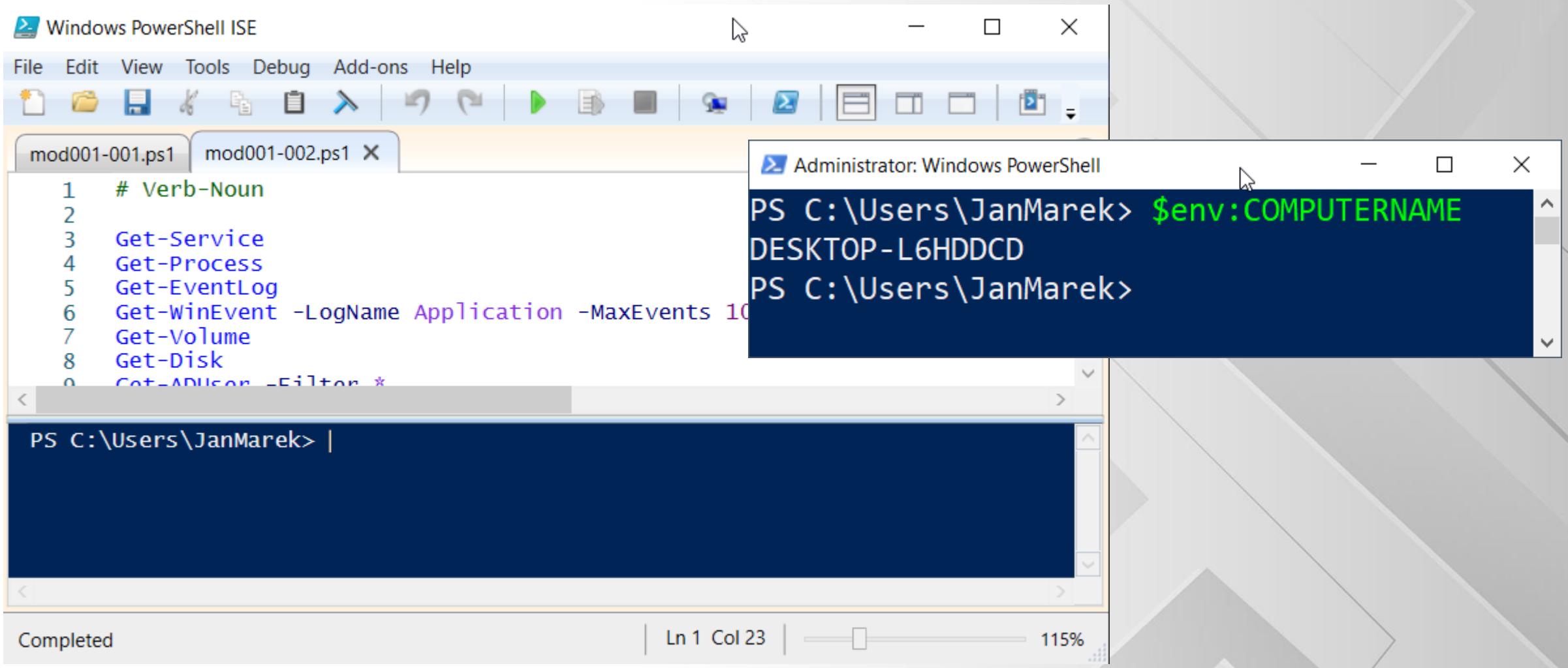
SOME EXAMPLES OF VERY USEFUL CMDLETS

- `# Verb-Noun`

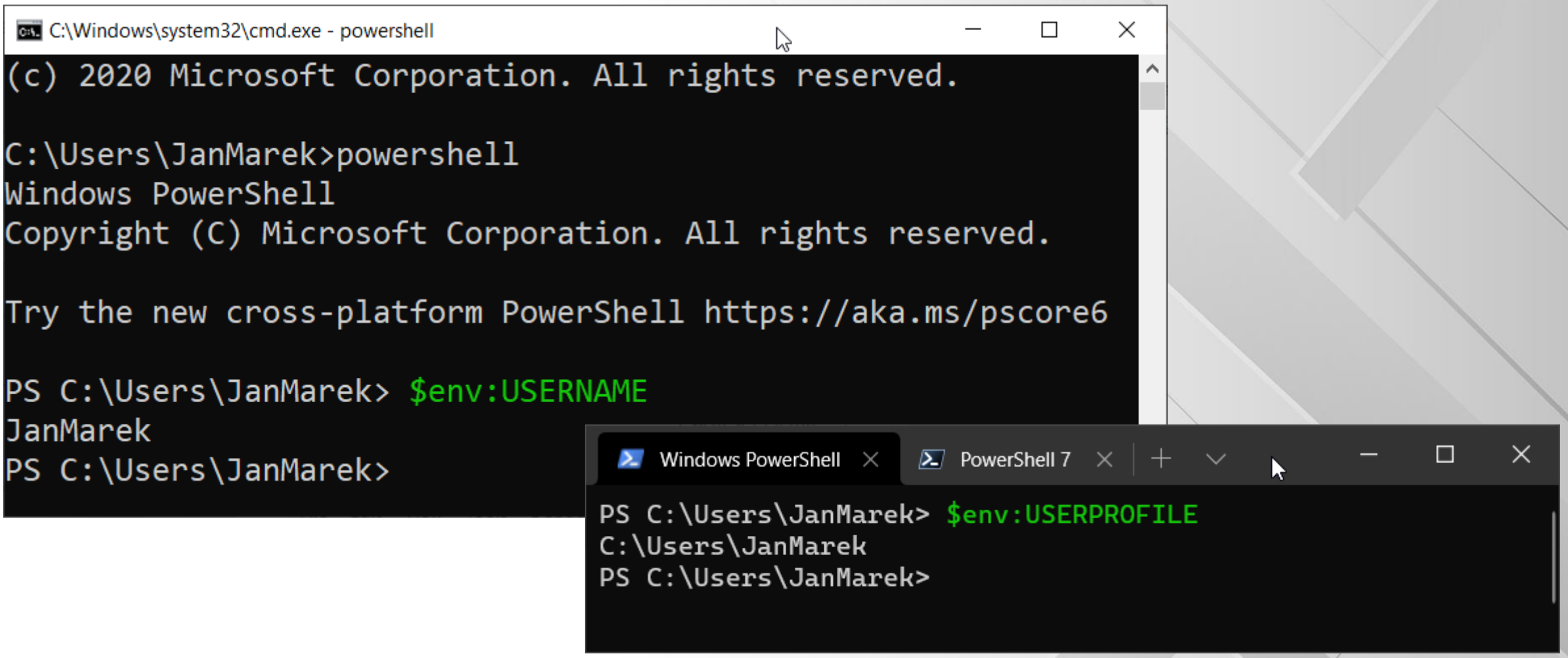
```
Out-File
Get-Service
Get-Process
Get-EventLog
Get-WinEvent -LogName Application -MaxEvents 10
Get-Volume
Get-Disk
Get-ADUser -Filter *
Set-Service -Name Spooler -StartupType Automatic
Get-Certificate
Get-DnsClientCache
Get-NetRoute
Get-NetIPAddress
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.1 -PrefixLength 24 -DefaultGateway 10.0.0.254
```

And so and so…

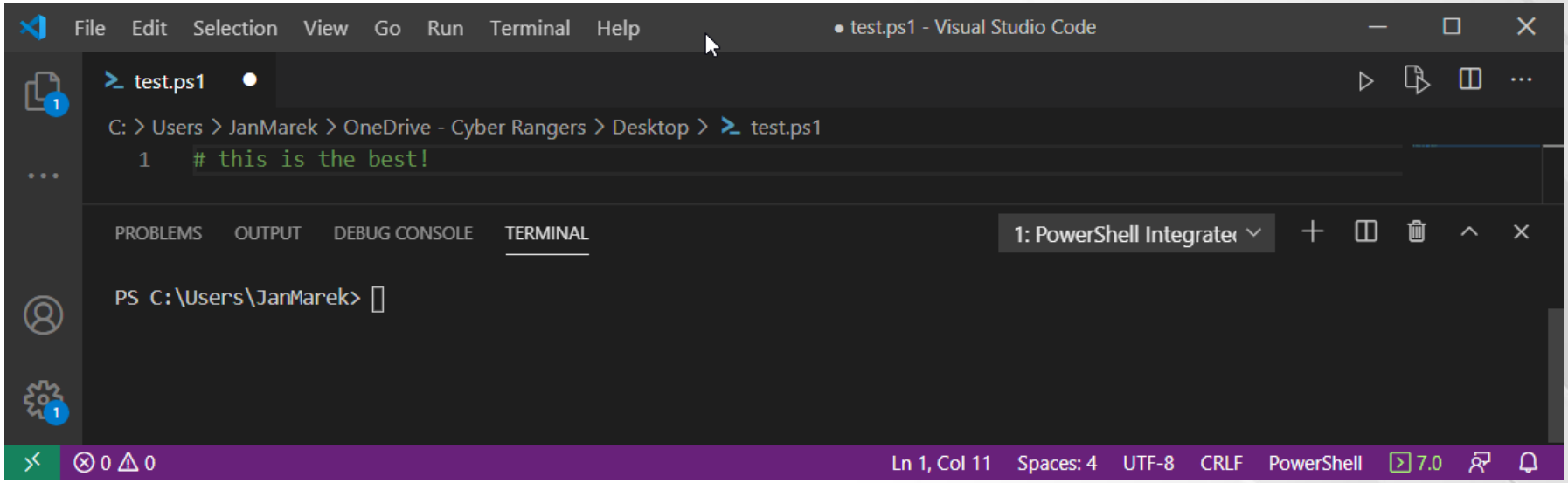
CONSOLE AND SCRIPT EDITORS (1/3)



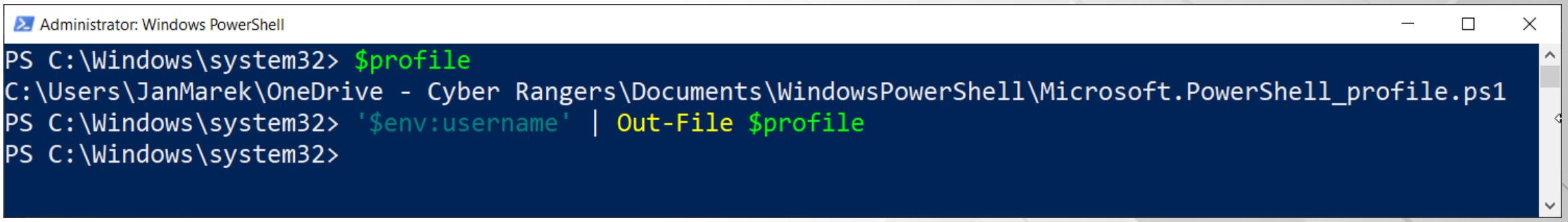
CONSOLE AND SCRIPT EDITORS (2/3)

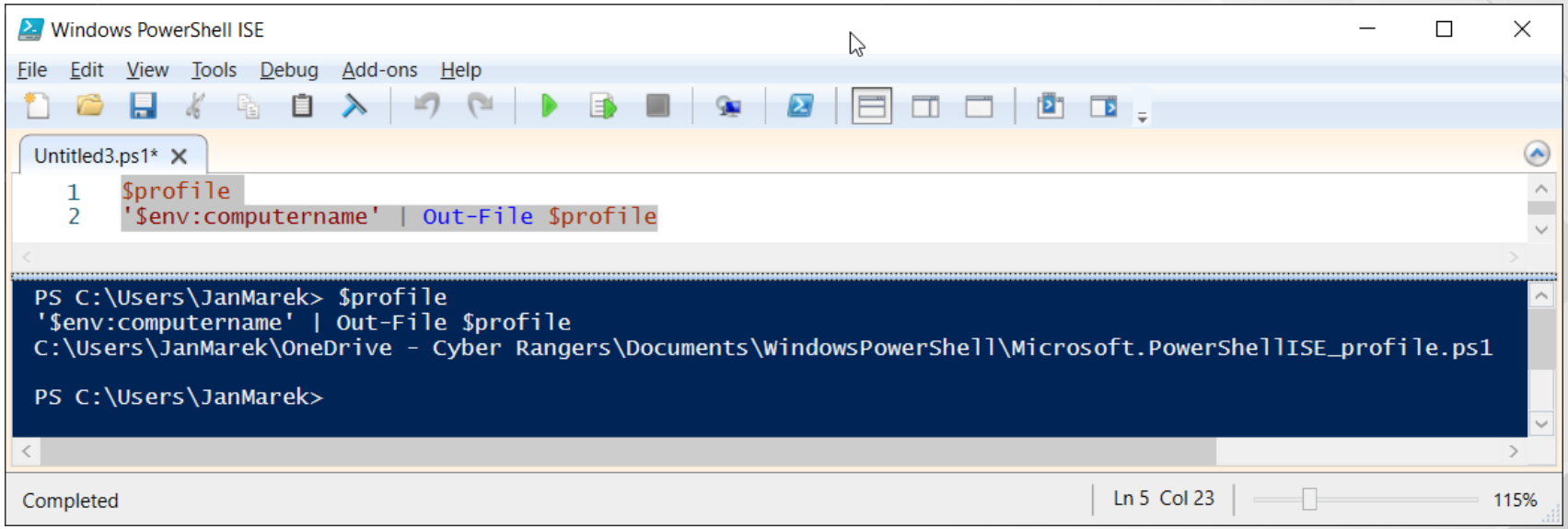


CONSOLE AND SCRIPT EDITORS (3/3)

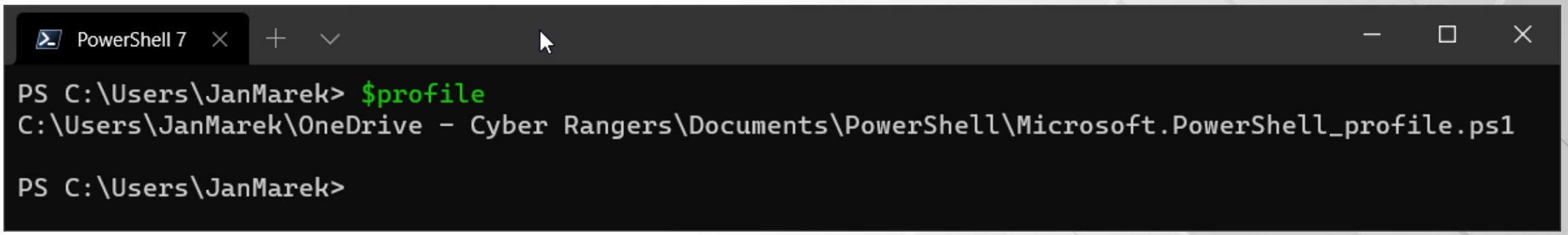


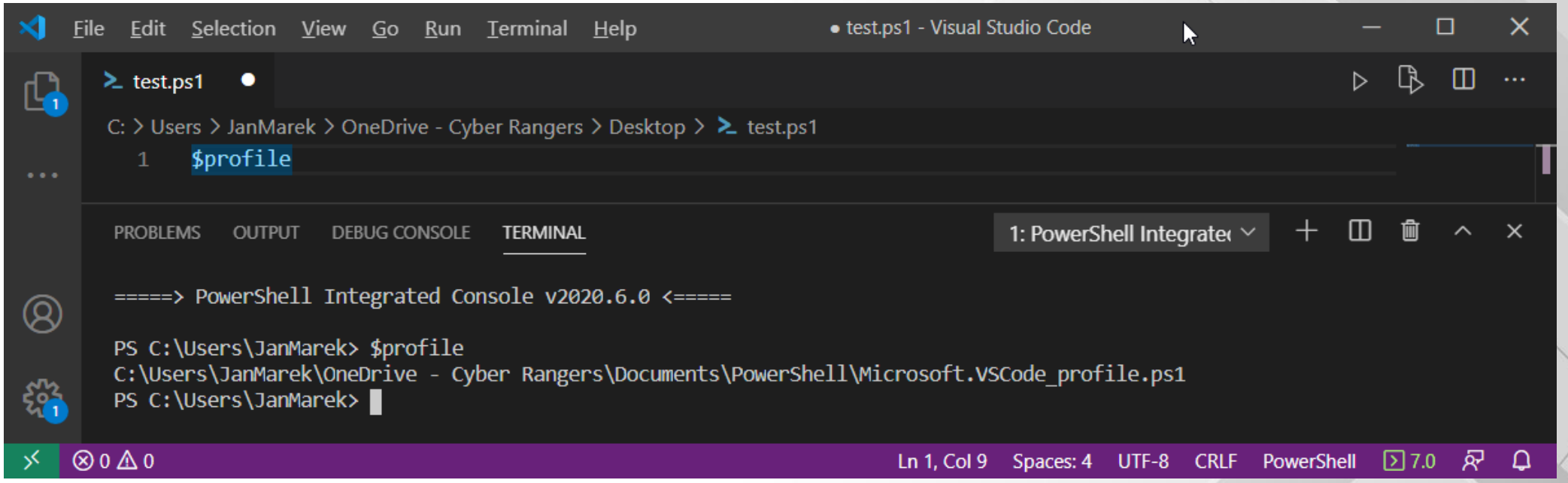
POWERSHELL PROFILE





POWERSHELL 7 PROFILE





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