

Under the Wire

The PowerShell training for the people

<https://www.underthewire.tech>

What is it?

Mission

Under the Wire trains experienced, developing, and novice information security professionals to use Windows PowerShell through innovative and fun wargames.

Objectives

- **Game play remains in the PowerShell command line environment or scripting environment. Add about SSH still uses PS Cmdline**
- **Game play emulates real interactions with PowerShell in Windows Enterprise environments or Windows based Small Office/Home Office (SOHO) Environments.**
- **Game play is engaging and challenging at specific levels of expertise.**
- **Game play promotes self-education without discouraging use of PowerShell.**

Heat Map



**Over 2000 Unique
Connections from 30
Countries in ~90 Days!**

Who are we?

The Under the Wire project was a collaboration between co-workers to bring the majesty of PowerShell to the public.

- **Peter Di Giorgio @DiGiorgio00**

- 18 years in the Department of Defense with 5 years of cyber security experience.
- Developed an appreciation for PowerShell, especially in large Windows enterprise networks

- **Fernando Tomlinson @Wired_Pulse**

- 17 years of forensics, incident response, and information technology experience with the Department of Defense
- PowerShell enthusiast; developing and coding in the language for 4 years

- **Alex Dierkes @StillWorthLess**

- Retired CW4 US Army, 20+ years in forensics, network analysis, incident response, and defense
- Got into PowerShell because I am lazy, hate repetitive tasks. 8 years experience

What do you need?

- **Your Computer**
- **Internet Connection**
- **Windows OS or SSH Client**



Figure 1: Hoope's Computer Science Lab. <http://hoopoe-tours.com/>

How does it Work?

- **Connect to SSID: underthewire**
- **Browse to: www.underthewire.tech**
- **Follow instructions for game connection**
- **From PowerShell**

1{

```
$webRequest = [Net.WebRequest]::Create("https://games.underthewire.tech:5986/wsman")  
try { $webRequest.GetResponse() } catch {}  
$cert = $webRequest.ServicePoint.Certificate  
$store = New-Object System.Security.Cryptography.X509Certificates.X509Store -ArgumentList "Root", "CurrentUser"  
$store.Open('ReadWrite') $store.Add($cert) $store.Close()  
Test-WSMan -ComputerName games.underthewire.tech -port 5986 -UseSSL
```


2{

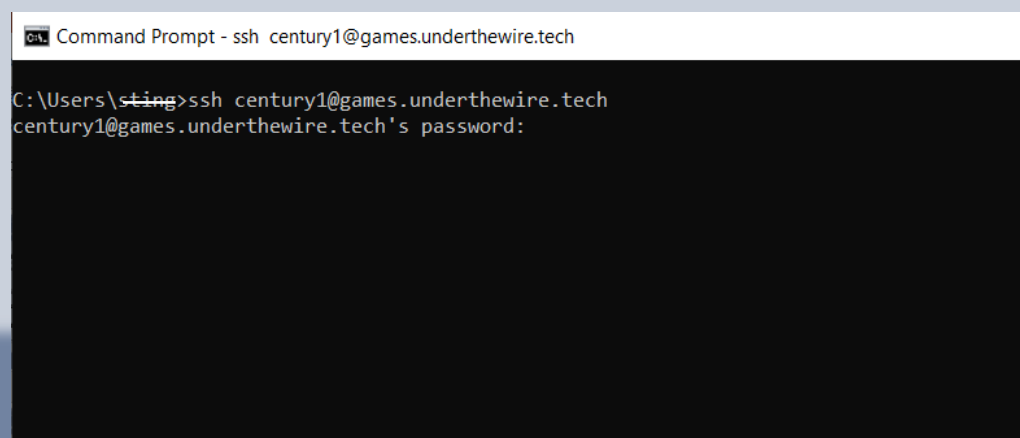
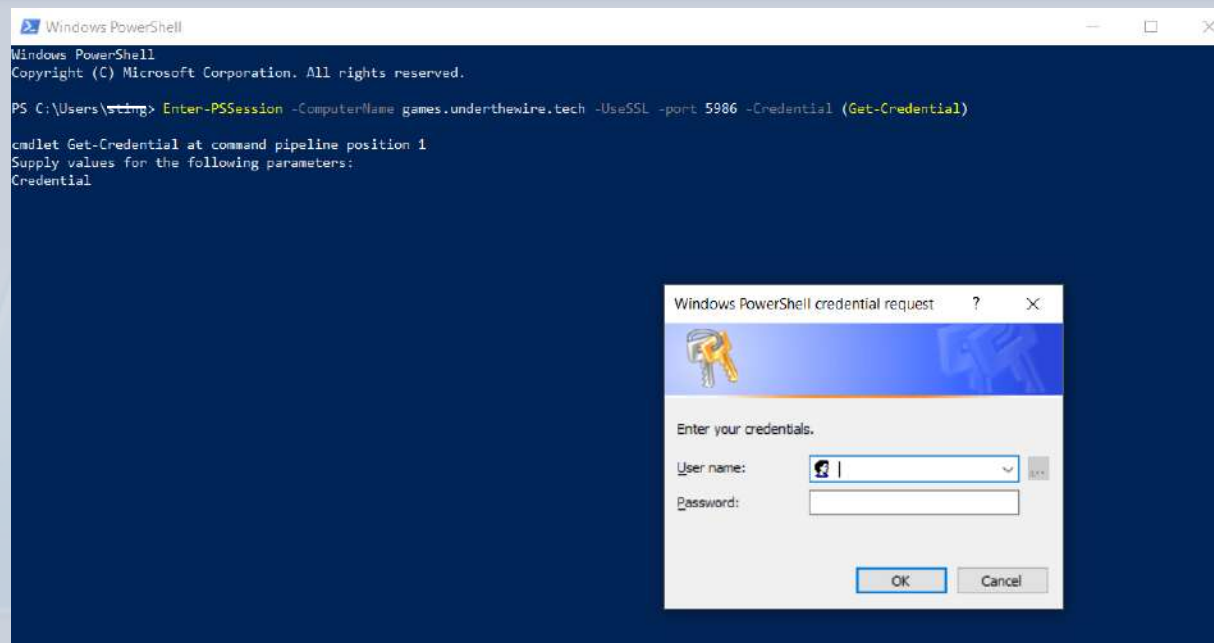
```
Enter-PSSession -ComputerName games.underthewire.tech -port 5986 -Credential (Get-Credential)
```

- **From SSH Client**

```
ssh workshop@games.underthewire.tech
```

Let's do this!

- **From Windows**
-  **Win + r**
- **Type “powershell”**
- **From a SSH Client**



Login

- **Login with workshop/workshop**
 - **ssh workshop@games.underthewire.tech**
 - **cd c:\users\century1\desktop**
 - **cd ..\century2\desktop**
 - **cd ..\trebek2\desktop**
- 

Website Demo



Get-Help

NAME

Get-Help

SYNOPSIS

Displays information about Windows PowerShell commands and concepts.

SYNTAX

Get-Help [[-Name] <String>] [-Category {Alias | Cmdlet | Provider | General | FAQ | Glossary | HelpFile | ScriptCommand | Function | Filter | ExternalScript | All | DefaultHelp | Workflow | DscResource | Class | Configuration}] [-Component <String[]>] -Detailed [-Functionality <String[]>] [-Path <String>] [-Role <String[]>] [<CommonParameters>]

DESCRIPTION

The **Get-Help** cmdlet displays information about Windows PowerShell concepts and commands, including cmdlets, functions, CIM commands, workflows, providers, aliases and scripts.

REMARKS

To see the examples, type: "get-help Get-Help -examples".

For more information, type: "get-help Get-Help -detailed".

For technical information, type: "get-help Get-Help -full".

For online help, type: "get-help Get-Help -online"

Windows PowerShell

PS C:\Users\sting> get-help help

NAME

Get-Help

SYNOPSIS

Displays information about Windows PowerShell commands and concepts.

Get-Command

NAME

Get-Command

SYNOPSIS

Gets all commands.

SYNTAX

Get-Command **[[-Name] <String[]>]** **[[-ArgumentList] <Object[]>]** **[-All]** **[-CommandType {Alias | Function | Filter | Cmdlet | ExternalScript | Application | Script | Workflow | Configuration | All}]** **[-FullyQualifiedModule <ModuleSpecification[]>]** **[-ListImported]** **[-Module <String[]>]** **[-ParameterName <String[]>]** **[-ParameterType <PSTypeName[]>]** **[-ShowCommandInfo]** **[-Syntax]** **[-TotalCount <Int32>]** **[<CommonParameters>]**

DESCRIPTION

The **Get-Command** cmdlet gets all commands that are installed on the computer, including cmdlets, aliases, functions, workflows, filters, scripts, and applications. **Get-Command** gets the commands from Windows PowerShell modules and snap-ins and commands that were imported from other sessions. To get only commands that have been imported into the current session, use the **ListImported** parameter.

REMARKS

To see the examples, type: "get-help Get-Command -examples".

For more information, type: "get-help Get-Command -detailed".

For technical information, type: "get-help Get-Command -full".

For online help, type: "get-help Get-Command -online"

Administrator: Windows PowerShell

PS C:\users\wolf> **Get-Help** Get-Command

NAME

Get-Command

SYNOPSIS

Gets all commands.

Get-Member

NAME

Get-Member

SYNOPSIS

Gets the properties and methods of objects.

SYNTAX

Get-Member **[[-Name] <String[]>] [-Force] [-InputObject <PSObject>] [-MemberType {AliasProperty | CodeProperty | Property | NoteProperty | ScriptProperty | Properties | PropertySet | Method | CodeMethod | ScriptMethod | Methods | ParameterizedProperty | MemberSet | Event | Dynamic | All}] [-Static] [-View {Extended | Adapted | Base | All}] [<CommonParameters>]**

DESCRIPTION

The Get-Member cmdlet gets the members, the properties and methods, of objects.

To specify the object, use the InputObject parameter or pipe an object to Get-Member . To get information about static members, the members of the class, not of the instance, use the Static parameter. To get only certain types of members, such as NoteProperties , use the MemberType parameter.

REMARKS

To see the examples, type: "get-help Get-Member -examples".

For more information, type: "get-help Get-Member -detailed".

For technical information, type: "get-help Get-Member -full".

For online help, type: "get-help Get-Member -online"

Administrator: Windows PowerShell

PS C:\users\wolf> **Get-Help** Get-Member

NAME

Get-Member

SYNOPSIS

Gets the properties and methods of objects.

Host

- **As a group we will go through four challenges.**
- **We will give you two minutes to complete the challenge then we will present the solution and answer.**
- **After these four challenges we will let you run for 10 minutes doing the challenges by yourself and at the end of the time we will go through the answers.**
- **During that time we will be walking around to provide assistance if you get stuck.**

Build Version

- **CENTURY 1**

- **What is the build version?**

- **NOTE:**

- **The format is as follows: **.******.*****
- **Include all periods**

Build Version

- **CENTURY 1**

- **What is the build version?**

- **NOTE:**

- **The format is as follows: **.******.*****
- **Include all periods**

2 Min

Build Version

- **CENTURY 1**

- **What is the build version?**

- **NOTE:**

- **The format is as follows: `**.******.***`**
- **Include all periods**

1.5 Min

Build Version

- **CENTURY 1**

- **What is the build version?**

- **NOTE:**

- **The format is as follows: **.******.*****
- **Include all periods**

1 Min

Build Version

- **CENTURY 1**

- **What is the build version?**

- **NOTE:**

- **The format is as follows: **.******.*****
- **Include all periods**

30 Sec

Build Version

- **Answer**

- **10.0.14393.693**

- **Solution**

PS C:\> \$psversiontable

PS C:\> \$psversiontable.buildversion

- **Powershell breaks up the build version...how do we bring them together?**

PS C:\> \$psversiontable.buildversion

- **“\$((\$psversiontable.buildversion.Major).\$(\$psversiontable.buildversion.Minor).\$(\$psversiontable.buildversion.Build).\$(\$psversiontable.buildversion.Revision))”**

Count Files

- **CENTURY 3**
- **Count the number of files on the user's desktop**



Count Files

- **CENTURY 3**
- **Count the number of files on the user's desktop**

2 Min

Count Files

- **CENTURY 3**
- **Count the number of files on the user's desktop**

1.5 Min

Count Files

- **CENTURY 3**
- **Count the number of files on the user's desktop**

1 Min

Count Files

- **CENTURY 3**
- **Count the number of files on the user's desktop**

30 Sec

Count Files

- **Answer**

- **919**

- **Solution**

PS C:\> (Get-ChildItem -file c:\users\century3\desktop).count



Count Directories

- **CENTURY 6**
- **Count the number of directories on the user's desktop.**



Count Directories

- **CENTURY 6**
- **Count the number of directories on the user's desktop.**

2 Min

Count Directories

- **CENTURY 6**
- **Count the number of directories on the user's desktop.**

1.5 Min

Count Directories

- **CENTURY 6**
- **Count the number of directories on the user's desktop.**

1 Min

Count Directories

- **CENTURY 6**
- **Count the number of directories on the user's desktop.**

30 Sec

Count Directories

- **Answer**

- **967**

- **Solution**

PS C:\> (Get-ChildItem -directory c:\users\century6\desktop).count



On Your Own

**Now you will do a couple of
sets of questions for 10/12
minutes each**

**After 10/12 minutes we will go
through the answers for each
section.**

Domain

- **Work on the following challenges:**

- **Oracle 5**

- **Oracle 13**

- **Ten minutes go**



Commands

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

**10 Min**

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

A black rounded rectangle with the text "5 Min" in orange, indicating a 5-minute duration.

5 Min

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands



1 Min

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Domain

• Oracle 5

- What is the name of the GPO that contains a description of "I_am_Groot"

• Answer

PS C:\> Get-help GPO

PS C:\> Get-GPO -All

- The description is where we want to find I_am_Groot

PS C:\> Get-GPO -All | Where-Object {\$_.Description -like 'i_am_groot'}

Under the Wire... PowerShell Training for the People!

```
PS C:\Users\Oracle5\documents> ((get-gpo -all | select DisplayName, Description  
| Where-Object {$_.Description -eq "I_am_Groot"}).DisplayName).tolower()
```

charlie

```
PS C:\Users\Oracle5\documents>
```

Domain

• Oracle 13

- What is the name of the user who created the Galaxy security group as depicted in the event logs on the desktop

• Answer

PS C:\> Set-Location C:\Users\Oracle13\Desktop

PS C:\> Get-WinEvent -Path .\security.evtx

- Looking for Windows Event ID for creation of a security group (4727)

PS C:\> Get-WinEvent -Path .\security.evtx | Where-Object {\$_.Id -eq '4727'}

```
PS C:\Users\Oracle13\Documents> Get-WinEvent -FilterHashTable @{Path="..\Desktop
/Security.evtx";ID="4727"} | Select *

Message                                     : A security-enabled global group was created.

Subject:
  Security ID:
S-1-5-21-2268727836-2773903800-2952248001-1621
  Account Name:
gamora
  Account Domain:
UNDERTHEWIRE
  Logon ID:
0xBC24FF
```

Application

- **Work on the following challenges:**

- **Oracle 8**

- **Groot 8**

- **Ten minutes go**



Commands

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands



10 Min

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

A black rounded rectangle with the text "5 Min" in a large, orange, sans-serif font. A large, light blue, semi-transparent arrow points from the center of the slide towards the bottom right, passing behind the timer graphic.

5 Min

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

**1 Min**

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Application

• Oracle 8

- What is the name of the file in the GET Request from www.guardian.galaxy.com within the log file on the desktop?

• Answer

PS C:\> Set-Location ..\desktop

- Then list what is in the directory (Get-ChildItem)

PS C:\> Get-content logs.txt

PS C:\> Get-content logs.txt | Select-string 'guardian.galaxy.com'

```
PS C:\Users\Oracle8\documents> get-content ../desktop/logs.txt | select-string 'guardian.galaxy.com'
```

```
guardian.galaxy.com - - [28/Jul/1995:13:03:55 -0400] "GET /images/star-lord.gif HTTP/1.0" 200 786
```

Application

• Groot 8

- What is the description of the firewall rule blocking MySQL

• Answer

PS C:\> Get-help firewallrule

PS C:\> Get-netfirewallrule

- As we see the displayname is where we want to find MySQL

PS C:\> Get-NetFirewallRule | Where-Object {\$_.DisplayName -like '*mysql*'}

```
PS C:\Users\Groot\documents> ((Get-NetFirewallRule | ?{$_.DisplayName -like '*MySQL*'}).description)
call_me
```

Break

BREAK TIME
15 Minutes

Registry/System

- **Work on the following challenges:**

- **Groot 1**
- **Oracle 1**
- **Oracle 12**

- **12 minutes go**



Commands

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

**12 Min**

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

A black rounded rectangle with the text "5 Min" in orange, indicating a 5-minute duration.

5 Min

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Commands

**1 Min**

- **Get-Command**
- **Get-Item**
- **Get-ChildItem**
- **Get-Content**
- **Get-AD....**
- **Get-DNS...**
- **Get-ItemProperty**
- **Get-WmiObject**
- **Get-NetFirewallRule**
- **Compare-Object**

- **Get-Help**
- **Get-Member**
- **Get-ComputerInfo**
- **Get-SmbShare**
- **Get-WinEvent**
- **Get-GPO**
- **Get-FileHash**
- **Get-AppLockerPolicy**
- **Select-String**
- **EventIDs: 4727,4699,4624,4722,4720,1102,4728**

- **[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(\$data))**
- **[System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String(\$data))**
- **[system.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes(\$data))**

Registry/System

• Groot 1

- What is the last five digits of the MD5 hash of this system's hosts file

• Answer

PS C:\> Get-Help Get-FileHash

PS C:\> Get-FileHash C:\windows\system32\drivers\etc\hosts -Algorithm MD5

PS C:\> (Get-FileHash C:\windows\system32\drivers\etc\hosts -Algorithm MD5).Hash

PS C:\> (Get-FileHash C:\windows\system32\drivers\etc\hosts `
-Algorithm MD5).Hash.substring(27,5)

Under the Wire... PowerShell Training for the People!

```
PS C:\Users\Groot1\documents> (get-filehash -Algorithm MD5 C:\windows\system32\drivers\etc\hosts).Hash.substring(27,5).tolower()  
464c3
```

Registry/System

• Oracle 1

- What is the timezone in which this system is set to

• Answer

PS C:\> Get-PSDrive

PS C:\> Get-Childitem HKLM:\System\CurrentControlSet\Control\TimezoneInformation

PS C:\> Get-ItemProperty HKLM:\System\CurrentControlSet\Control\TimezoneInformation

PS C:\> (Get-ItemProperty HKLM:\System\CurrentControlSet\Control\TimezoneInformation).TimeZoneKeyName

```
PS C:\Users\Oracle1\documents> (get-itemproperty hklm:\system\currentcontrolset\
control\timezoneinformation).TimeZoneKeyName
UTC
```

Registry/System

• Oracle 12

- What is the IP of the system that this user has previously established a remote desktop with

• Answer

PS C:\> Get-PSDrive

PS C:\> Get-ChildItem "HKCU:\software\microsoft\terminal server client"

PS C:\> (Get-ChildItem "HKCU:\software\microsoft\terminal server client")

PS C:\> (Get-ChildItem "HKCU:\software\microsoft\terminal server client").pschildname

```
PS C:\Users\Oracle12\documents> ((Get-ChildItem "HKCU:\software\microsoft\terminal server client").Name).split("\")[4]
192.168.2.3
```


PoshHunter

PoSh Hunter

[News](#)

[Challenges](#)

[Scoreboard](#)

[Help](#)

[Admin](#)

[Statistics](#)

[Profile](#)

[Logout](#)

Welcome to PoSh Hunter!

Are Your PowerShell Skills Strong Enough to Survive?



Thank you for joining us!!!

<http://www.underthewire.tech>

Give prizes.....