**Windows PowerShell**

* Version:
  + (Get-Host).Version
  + Get-Host
  + $host.Version
  + $host
  + $PSVersionTable

Text

Description automatically generated

Diagram

Description automatically generated

What is the location of the file "interesting-file.txt"

* Command:
  + Get-Childitem -path C:\ -recurse -erroraction silentlycontinue -include \*interesting-file.txt\*
  + <https://devblogs.microsoft.com/scripting/use-windows-powershell-to-search-for-files/>
* Answer:
  + C:\Program Files

Specify the contents of this file

* Command:
  + Start “C:\Program Files\interesting-file.txt.txt”
* Answer:
  + Notsointerestingcontent

What is the location of the file "interesting-file.txt"

* Command:
  + Get-Command | Where-Object -property CommandType -eq cmdlet | measure-object
* Answer:
  + 6638

Get the MD5 hash of interesting-file.txt

* Command:
  + Get-filehash -algorithm md5 -path “C:\Program Files\interesting-file.txt.txt”
* Answer:
  + 49A586A2A9456226F8A1B4CEC6FAB329

What is the command to get the current working directory?

* Command and Answer:
  + Get-location

Does the path "C:\Users\Administrator\Documents\Passwords" Exist(Y/N)?

* Command:
  + Test-path -path “C:\Users\Administrator\Documents\Passwords”
  + <https://adamtheautomator.com/powershell-check-if-file-exists/>
* Answer:
  + No

What command would you use to make a request to a web server?

* Command and Answer:
  + Invoke-WebRequest
  + <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-webrequest?view=powershell-7.3>

Base64 decode the file b64.txt on Windows.

* Command:
  + certutil -decode "C:\Users\Administrator\Desktop\b64.txt" decode.txt
  + <https://medium.com/@CyberOPS.LittleDog/tryhackme-hacking-with-powershell-834d8b86ec4a>
* Answer:
  + Ihopeyoudidthisonwindows

**Enumeration:**

How many users are there on the machine?

* Command:
  + Get-localuser | measure-object
* Answer:
  + 5

Which local user does this SID(S-1-5-21-1394777289-3961777894-1791813945-501) belong to?

* Command:
  + Get-LocalUser | Select-Object SID, NAME
* Answer:
  + Guest

How many local groups exist?

* Command:
  + Get-localgroup | measure-object
* Answer:
  + 24

What command did you use to get the IP address info?

* Command and answer:
  + Get-netipaddress

How many ports are listed as listening?

* Command:
  + Get-nettcpconnection -state listen | measure-object
  + <https://adamtheautomator.com/netstat-port/>
* Answer:
  + 20

What is the remote address of the local port listening on port 445?

* Command:
  + Get-nettcpconnection | where-object -property localport -match 445
* Answer:
  + ::

How many patches have been applied?

* Command:
  + Get-hotfix | measure-object
* Answer:
  + 20
  + <https://learnxinyminutes.com/docs/powershell/>

When was the patch with ID KB4023834 installed?

* Command:
  + Get-hotfix | where-object -property HotFixID -match KB4023834
* Answer:
  + 6/15/2017 12:00:00 AM

Find the contents of a backup file.

* Command:
  + Get-childitem -path c:\ -recurse -erroraction silentlycontinue | where-object -property Name -match bak | get-content
* Answer:
  + Backpassflag
  + <https://ratiros01.medium.com/tryhackme-hacking-with-powershell-bf6dbc5febc9>

Search for all files containing API\_KEY

* Command:
  + Get-childitem -path C: -recurse | select-string -pattern API\_KEY -CaseSensitive
* Answer:
  + Fakekey123

What command do you do to list all the running processes?

* Command and Answer:
  + Get-process
  + <https://sid-500.com/2017/07/25/powershell-cmdlets-list-all-availabe-parameters-without-using-the-help/>

What is the path of the scheduled task called new-sched-task?

* Command:
  + Get-scheduledtask -taskpath \
* Answer:
  + /

Who is the owner of the C:\ ?

* Command:
  + Get-acl C:\
* Answer:
  + NT SERVICE\TrustedInstaller

**Basic Scripting Challenge**

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_comparison_operators?view=powershell-7.3&viewFallbackFrom=powershell-6>

What file contains the password?

* Command:
  + Get-childitem -recurse | select-string -pattern password
* Answer:
  + Doc3M.txt

What is the password?

* Command:
  + Same as above
* Answer:
  + Johnisalegend99

What files contains an HTTPS link?

* Command:
  + Get-childitem -recurse | select-string -pattern https
* Answer:
  + Doc2Mary

**Intermediate Scripting**

<https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-how-to-scan-open-ports-within-a-network/ba-p/924149>

A picture containing chart

Description automatically generated

$range = (130..140)

$network = (10.10.100.116)

foreach($ran in $range)

{

test-netconnection $network -port $ran -ErrorAction SilentlyContinue

}

How many open ports did you find between 130 and 140(inclusive of those two)?

* Answer:
  + 11