Hacking With Powershell

www.tryhackme.com

by:g4mbit5

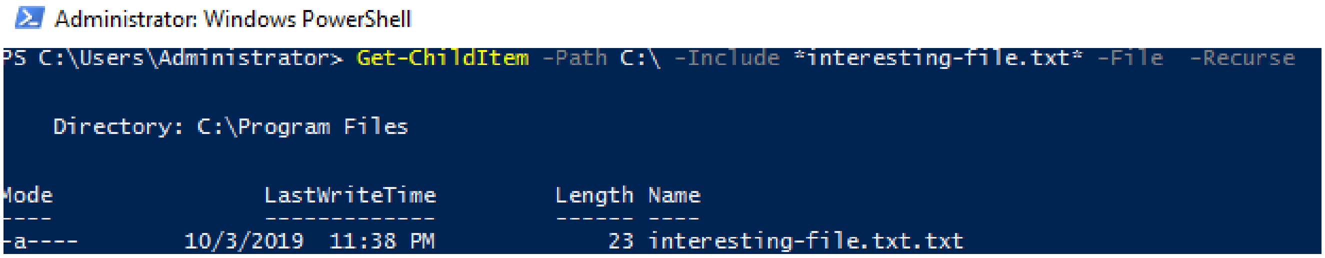
Task 2: What is Powershell?

Get-Help

Task 3: Basic Powershell Commands

Question #1

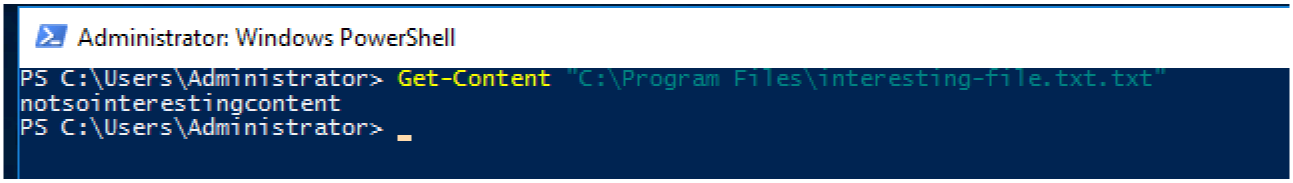
```
Get-ChildItem -Path C:\ -Include *interesting-file.txt* -File -Recurse -ErrorAction SilentlyContinue
```



```
PS C:\Users\Administrator> Get-ChildItem -Path C:\ -Include *interesting-file.txt* -File  -Recurse


    Directory: C:\Program Files


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/3/2019  11:38 PM             23 interesting-file.txt.txt
```

Question #2

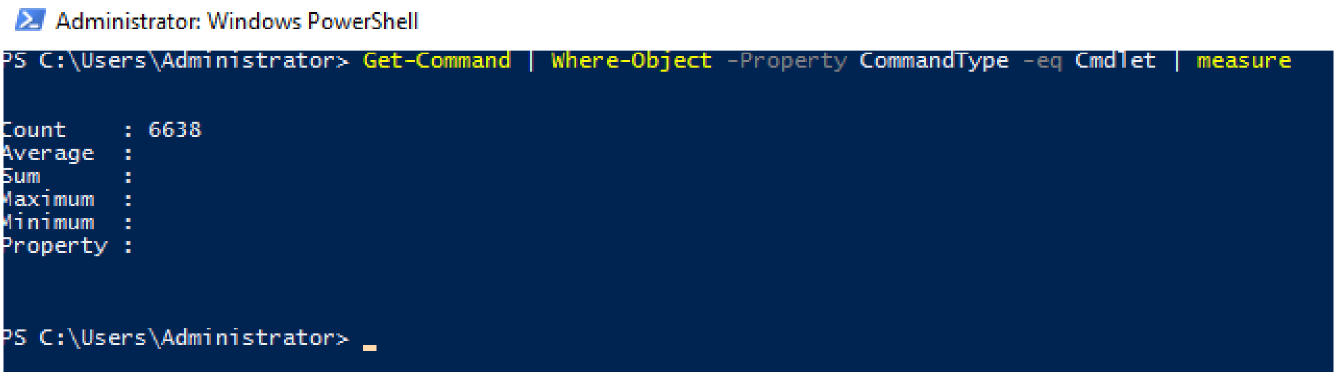
```
Get-Content "C:\Program Files\interesting-file.txt.txt"
```



```
PS C:\Users\Administrator> Get-Content "C:\Program Files\interesting-file.txt.txt"
notsointerestingcontent
PS C:\Users\Administrator> _
```

Question #3

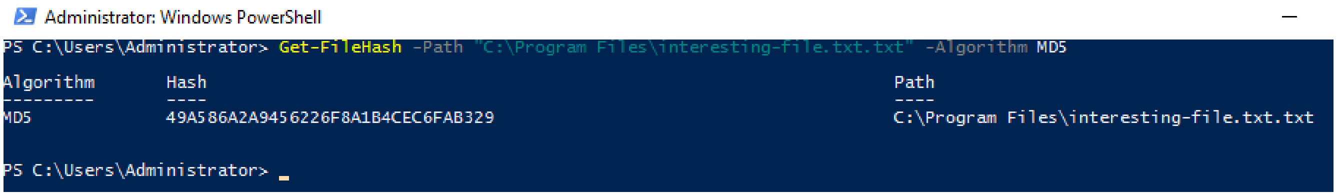
```
Get-Command | Where-Object -Property CommandType -eq Cmdlet | measure
```



```
PS C:\Users\Administrator> Get-Command | Where-Object -Property CommandType -eq Cmdlet | measure


Count    : 6638
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Users\Administrator> _
```

Question #4

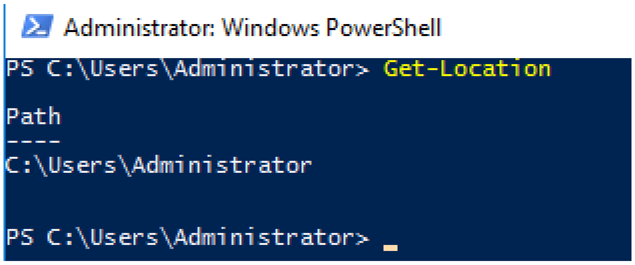
Get-FileHash -Path “C:\Program Files\interesting-file.txt.txt” -Algorithm MD5



```
PS C:\Users\Administrator> Get-FileHash -Path "C:\Program Files\interesting-file.txt.txt" -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             49A586A2A9456226F8A1B4CEC6FAB329                                       C:\Program Files\interesting-file.txt.txt


PS C:\Users\Administrator> _
```

Question#5

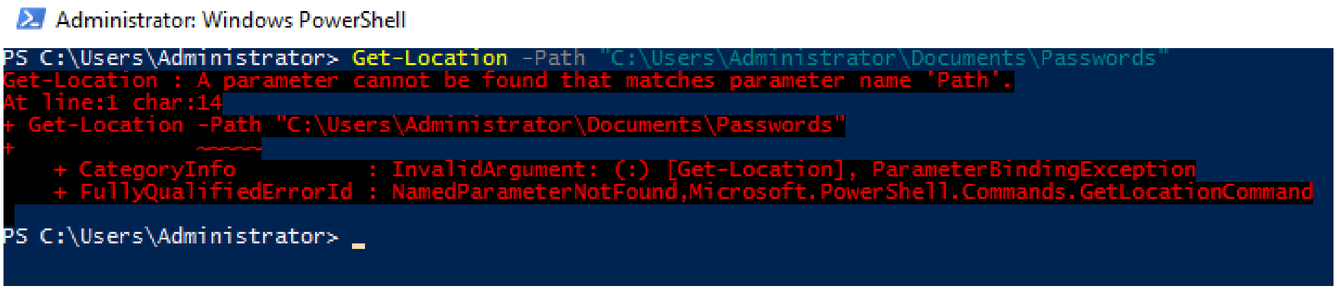
Get-Location



```
PS C:\Users\Administrator> Get-Location

Path
----
C:\Users\Administrator


PS C:\Users\Administrator> _
```

Question #6

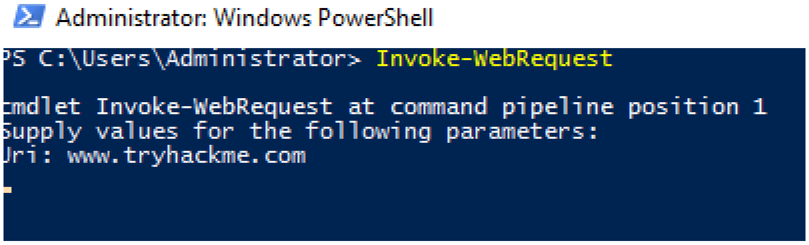
```
Get-Location -Path "C:\Users\Administrator\Documents\Passwords"
```



```
PS C:\Users\Administrator> Get-Location -Path "C:\Users\Administrator\Documents\Passwords"
Get-Location : A parameter cannot be found that matches parameter name 'Path'.
At line:1 char:14
+ Get-Location -Path "C:\Users\Administrator\Documents\Passwords"
+              ~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Get-Location], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.GetLocationCommand

PS C:\Users\Administrator> _
```

Question # 7

`Invoke-WebRequest`

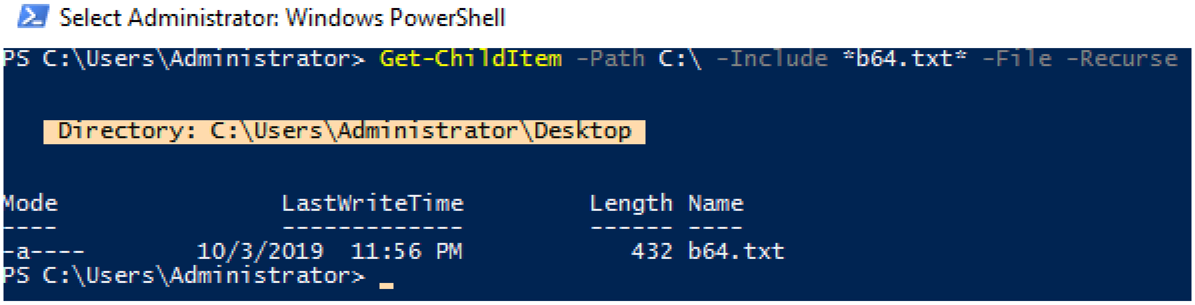


```
PS C:\Users\Administrator> Invoke-WebRequest

cmdlet Invoke-WebRequest at command pipeline position 1
Supply values for the following parameters:
Uri: www.tryhackme.com
```

Question # 8

Circle back to step 1 to find the file path first.

Get-ChildItem -Path C:\ -Include *b64.txt* -File -Recurse

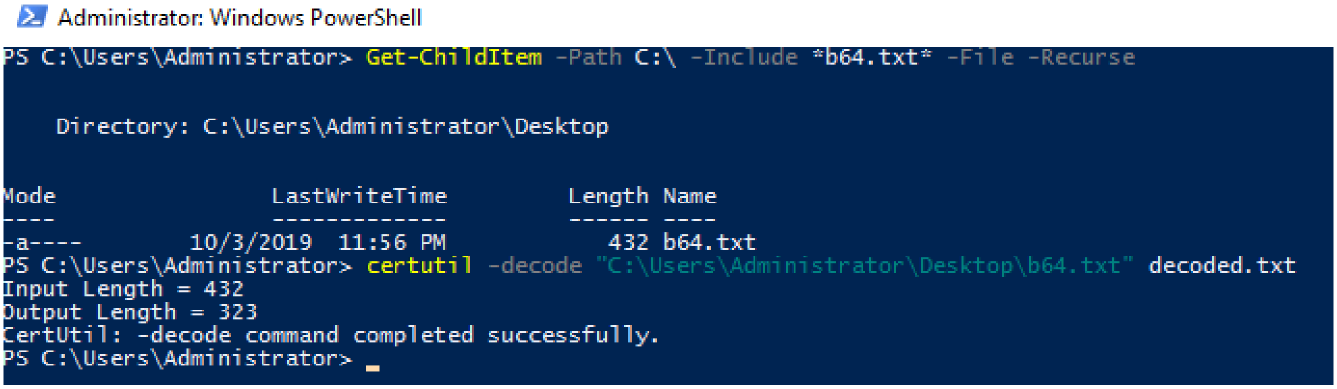


```
PS C:\Users\Administrator> Get-ChildItem -Path C:\ -Include *b64.txt* -File -Recurse


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/3/2019  11:56 PM            432 b64.txt
PS C:\Users\Administrator> _
```

**After it finds the file just hit Ctrl^C to end the command.

Then use:

`certutil -decode "C:\Users\Administrator\Desktop\b64.txt" decoded.txt`



```
PS C:\Users\Administrator> Get-ChildItem -Path C:\ -Include *b64.txt* -File -Recurse


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/3/2019  11:56 PM            432 b64.txt
PS C:\Users\Administrator> certutil -decode "C:\Users\Administrator\Desktop\b64.txt" decoded.txt
Input Length = 432
Output Length = 323
CertUtil: -decode command completed successfully.
PS C:\Users\Administrator> _
```

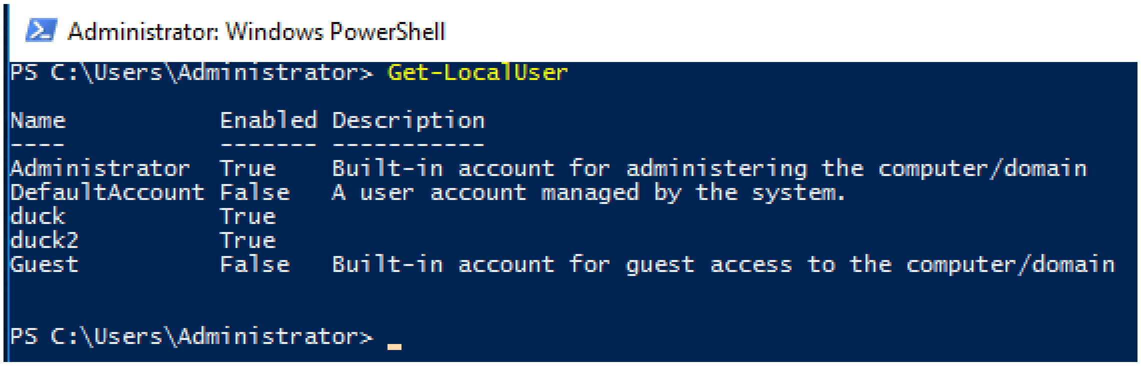
Then type:

Get-Content decoded.txt to show the flag.

Task 4: Enumeration

Question #1

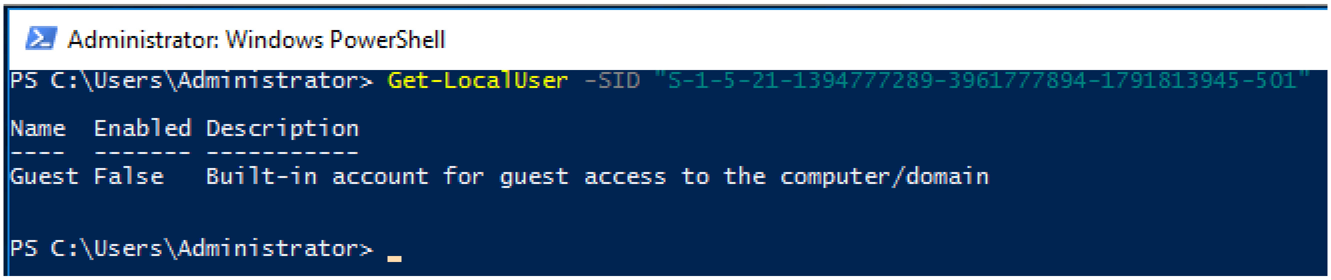
```
Get-LocalUser
```



```
PS C:\Users\Administrator> Get-LocalUser

Name           Enabled Description
----           ------- -----------
Administrator  True    Built-in account for administering the computer/domain
DefaultAccount False   A user account managed by the system.
duck           True
duck2          True
Guest          False   Built-in account for guest access to the computer/domain


PS C:\Users\Administrator> _
```

Question #2

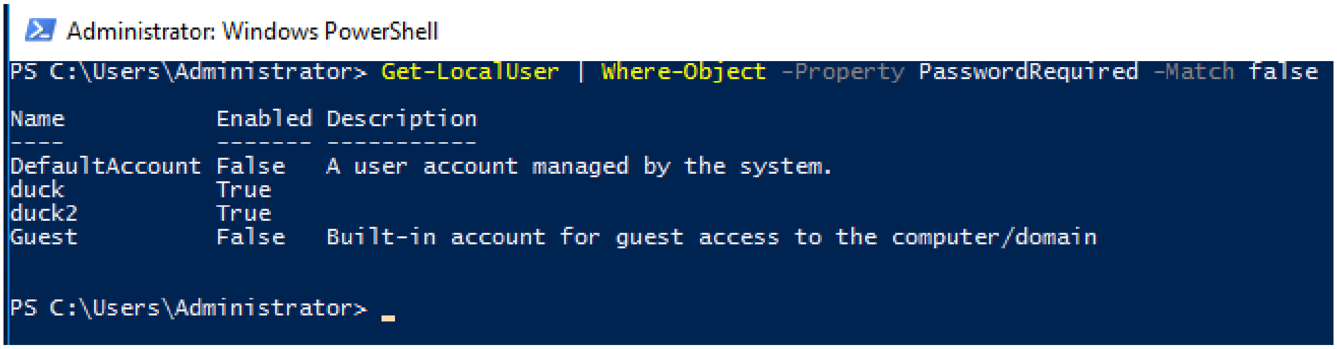
```
Get-Command Get-LocalUser -SID “S-1-5-21-1394777289-3961777894-1791813945-501”
```



```
PS C:\Users\Administrator> Get-LocalUser -SID "S-1-5-21-1394777289-3961777894-1791813945-501"

Name  Enabled Description
----  ------- -----------
Guest False   Built-in account for guest access to the computer/domain


PS C:\Users\Administrator> _
```

Question #3

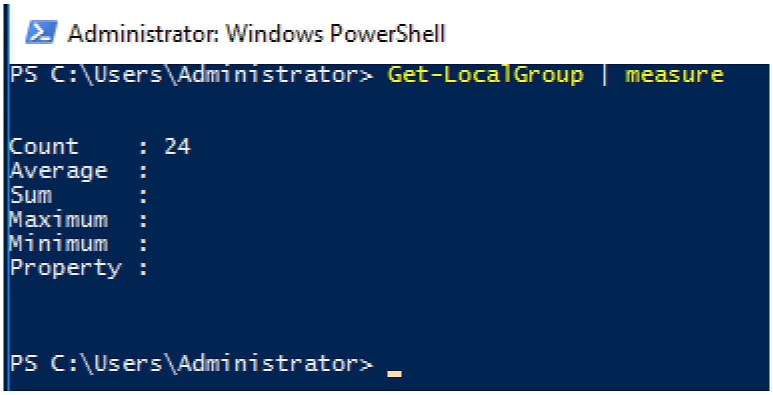
```
Get-LocalUser | Where-Object -Property PasswordRequired -Match false
```



```
PS C:\Users\Administrator> Get-LocalUser | Where-Object -Property PasswordRequired -Match false

Name           Enabled Description
----           ------- -----------
DefaultAccount False   A user account managed by the system.
duck           True
duck2          True
Guest          False   Built-in account for guest access to the computer/domain


PS C:\Users\Administrator> _
```

Question #4

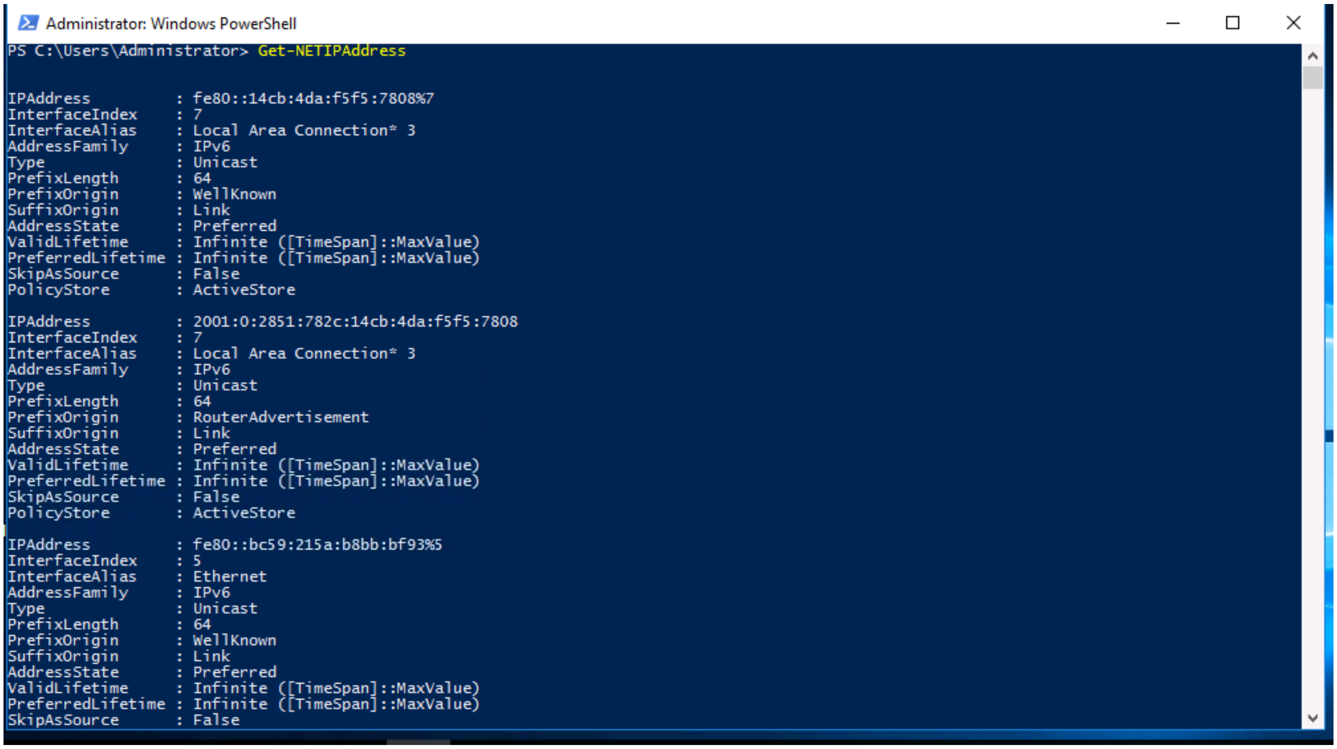
Get-LocalGroup | measure



```
PS C:\Users\Administrator> Get-LocalGroup | measure


Count    : 24
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Users\Administrator> _
```

Question #5

`Get-NetIPAddress`

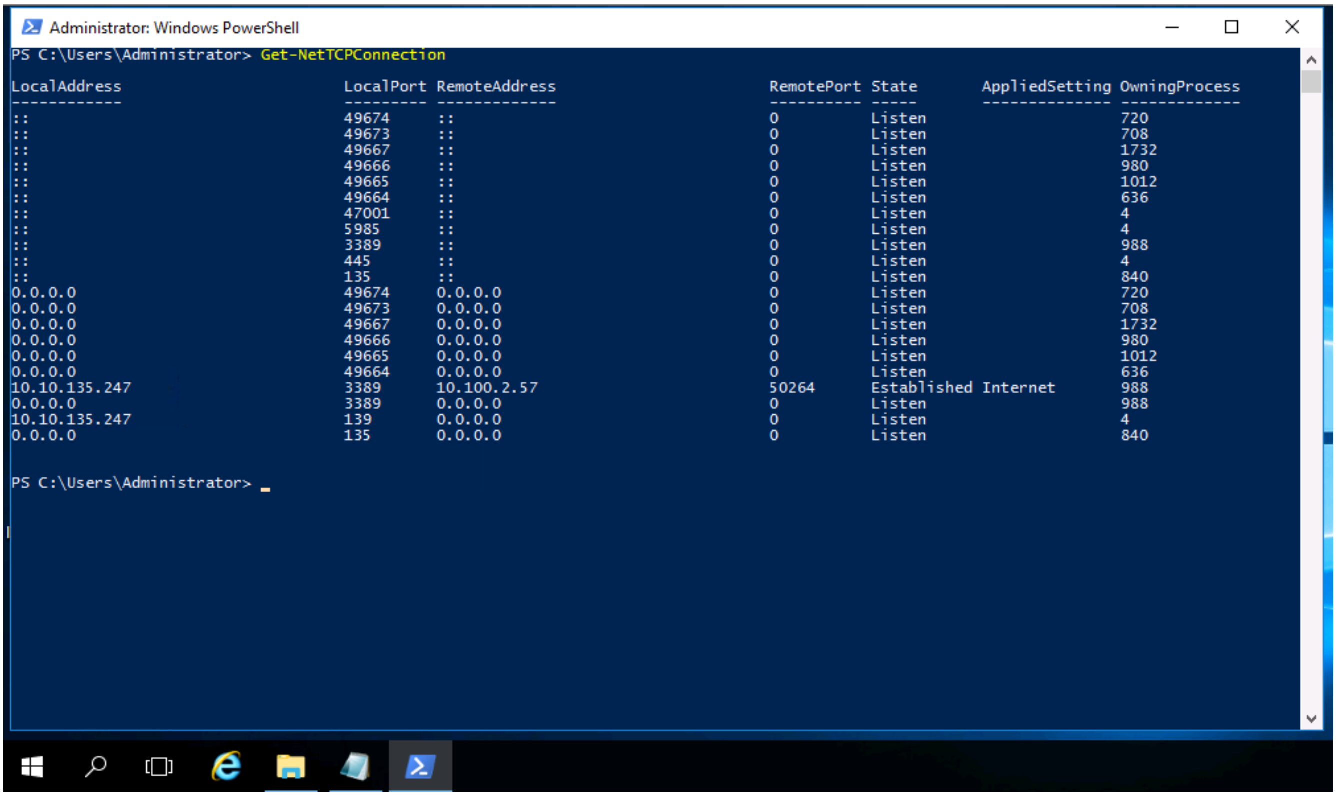


```
PS C:\Users\Administrator> Get-NETIPAddress


IPAddress         : fe80::14cb:4da:f5f5:7808%7
InterfaceIndex    : 7
InterfaceAlias    : Local Area Connection* 3
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 2001:0:2851:782c:14cb:4da:f5f5:7808
InterfaceIndex    : 7
InterfaceAlias    : Local Area Connection* 3
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : RouterAdvertisement
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : fe80::bc59:215a:b8bb:bf93%5
InterfaceIndex    : 5
InterfaceAlias    : Ethernet
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
```

Question # 6

To just list the ports which is handy if you need to see all connections and who is talking to who.

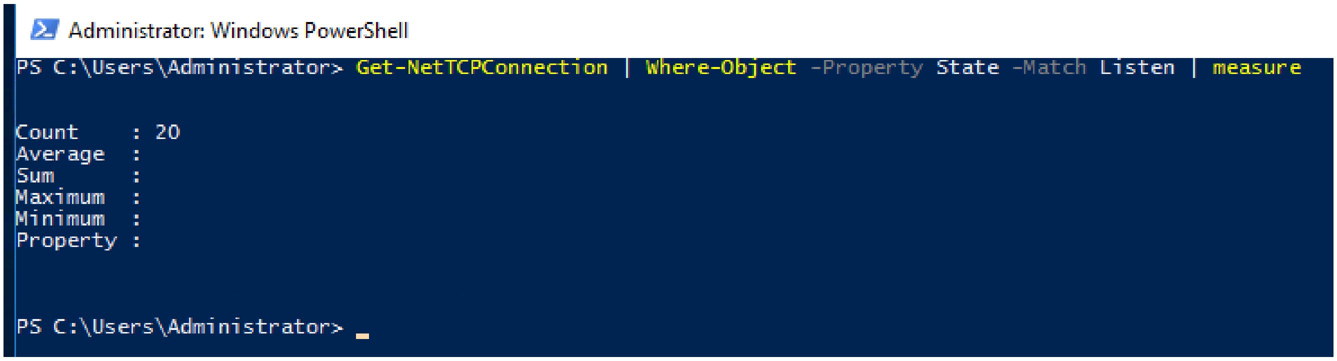
```
Get-NetTCPConnection
```



```
PS C:\Users\Administrator> Get-NetTCPConnection

LocalAddress                        LocalPort RemoteAddress                       RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                       ---------- -----       -------------- -------------
::                                  49674     ::                                  0          Listen                     720
::                                  49673     ::                                  0          Listen                     708
::                                  49667     ::                                  0          Listen                     1732
::                                  49666     ::                                  0          Listen                     980
::                                  49665     ::                                  0          Listen                     1012
::                                  49664     ::                                  0          Listen                     636
::                                  47001     ::                                  0          Listen                     4
::                                  5985      ::                                  0          Listen                     4
::                                  3389      ::                                  0          Listen                     988
::                                  445       ::                                  0          Listen                     4
::                                  135       ::                                  0          Listen                     840
0.0.0.0                             49674     0.0.0.0                             0          Listen                     720
0.0.0.0                             49673     0.0.0.0                             0          Listen                     708
0.0.0.0                             49667     0.0.0.0                             0          Listen                     1732
0.0.0.0                             49666     0.0.0.0                             0          Listen                     980
0.0.0.0                             49665     0.0.0.0                             0          Listen                     1012
0.0.0.0                             49664     0.0.0.0                             0          Listen                     636
10.10.135.247                       3389      10.100.2.57                         50264      Established Internet       988
0.0.0.0                             3389      0.0.0.0                             0          Listen                     988
10.10.135.247                       139       0.0.0.0                             0          Listen                     4
0.0.0.0                             135       0.0.0.0                             0          Listen                     840


PS C:\Users\Administrator> _
```

```
To total the listening connections up use.
```

```
GEt-NetTCPConnection | Where-Object -Property State -Match Listen | measure
```



```
PS C:\Users\Administrator> Get-NetTCPConnection | Where-Object -Property State -Match Listen | measure


Count    : 20
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Users\Administrator> _
```

Question #7

The answer is

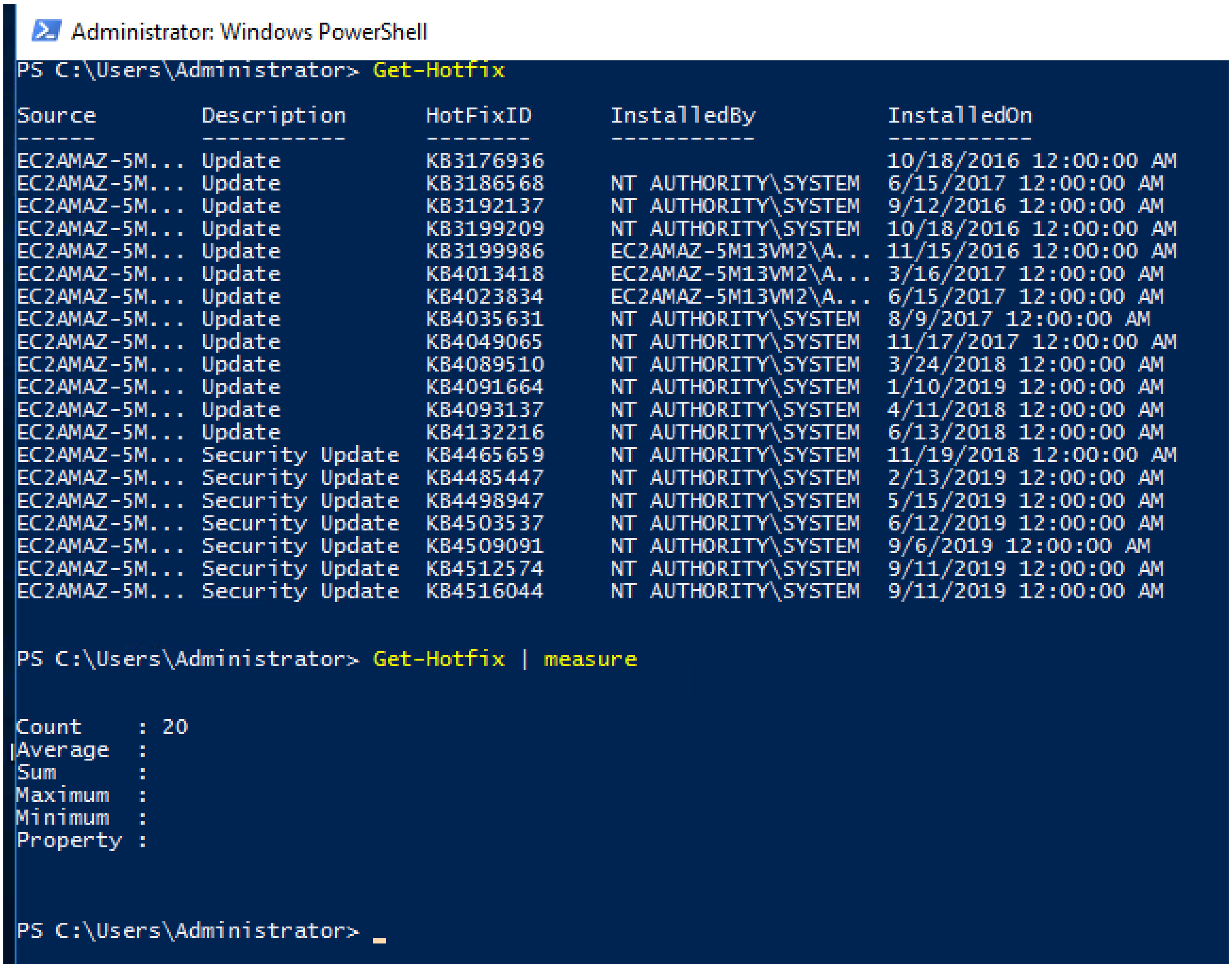
::

Ummmm, Yeeeah. Anyways, moving on from that nonsense.

Question #8

Again, to list things out when you need to see the values.

Get-Hotfix



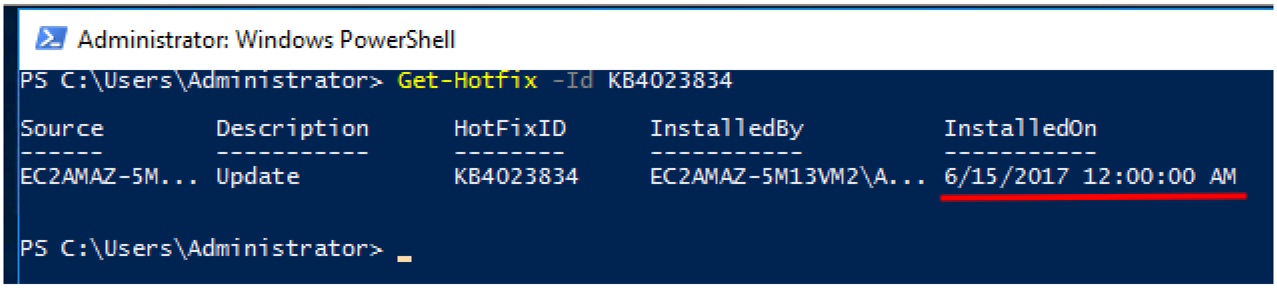
```
PS C:\Users\Administrator> Get-Hotfix

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
EC2AMAZ-5M... Update           KB3176936                          10/18/2016 12:00:00 AM
EC2AMAZ-5M... Update           KB3186568     NT AUTHORITY\SYSTEM  6/15/2017 12:00:00 AM
EC2AMAZ-5M... Update           KB3192137     NT AUTHORITY\SYSTEM  9/12/2016 12:00:00 AM
EC2AMAZ-5M... Update           KB3199209     NT AUTHORITY\SYSTEM  10/18/2016 12:00:00 AM
EC2AMAZ-5M... Update           KB3199986     EC2AMAZ-5M13VM2\A... 11/15/2016 12:00:00 AM
EC2AMAZ-5M... Update           KB4013418     EC2AMAZ-5M13VM2\A... 3/16/2017 12:00:00 AM
EC2AMAZ-5M... Update           KB4023834     EC2AMAZ-5M13VM2\A... 6/15/2017 12:00:00 AM
EC2AMAZ-5M... Update           KB4035631     NT AUTHORITY\SYSTEM  8/9/2017 12:00:00 AM
EC2AMAZ-5M... Update           KB4049065     NT AUTHORITY\SYSTEM  11/17/2017 12:00:00 AM
EC2AMAZ-5M... Update           KB4089510     NT AUTHORITY\SYSTEM  3/24/2018 12:00:00 AM
EC2AMAZ-5M... Update           KB4091664     NT AUTHORITY\SYSTEM  1/10/2019 12:00:00 AM
EC2AMAZ-5M... Update           KB4093137     NT AUTHORITY\SYSTEM  4/11/2018 12:00:00 AM
EC2AMAZ-5M... Update           KB4132216     NT AUTHORITY\SYSTEM  6/13/2018 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4465659     NT AUTHORITY\SYSTEM  11/19/2018 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4485447     NT AUTHORITY\SYSTEM  2/13/2019 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4498947     NT AUTHORITY\SYSTEM  5/15/2019 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4503537     NT AUTHORITY\SYSTEM  6/12/2019 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4509091     NT AUTHORITY\SYSTEM  9/6/2019 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4512574     NT AUTHORITY\SYSTEM  9/11/2019 12:00:00 AM
EC2AMAZ-5M... Security Update  KB4516044     NT AUTHORITY\SYSTEM  9/11/2019 12:00:00 AM


PS C:\Users\Administrator> Get-Hotfix | measure


Count    : 20
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Users\Administrator> _
```

To total them up.

Get-Hotfix | measure

Question #9

```
Get-Hotfix -Id KB4023834
```



```
PS C:\Users\Administrator> Get-Hotfix -Id KB4023834

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
EC2AMAZ-5M... Update           KB4023834     EC2AMAZ-5M13VM2\A... 6/15/2017 12:00:00 AM


PS C:\Users\Administrator> _
```

Question #10

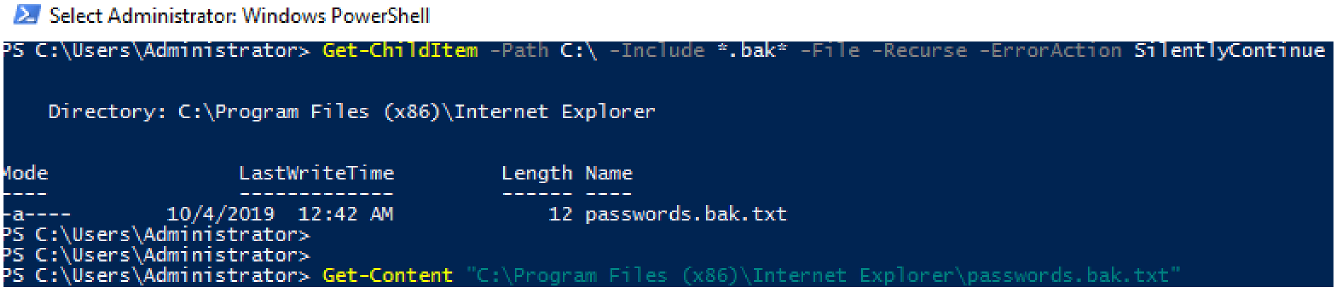
Circle again back to the very first command.

To get the path first:

```
Get-ChildItem -Path C:\ -Include *.bak* -File -Recurse -ErrorAction
SilentlyContinue
```

Then use the path to get the contents:

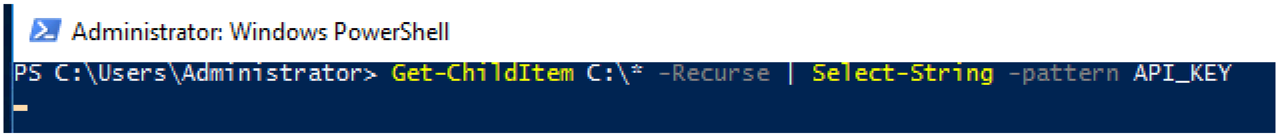
```
Get-Content “C:\Program Files (x86)\Internet Explorer\passwords.bak.txt”
```



```
PS C:\Users\Administrator> Get-ChildItem -Path C:\ -Include *.bak* -File -Recurse -ErrorAction SilentlyContinue


    Directory: C:\Program Files (x86)\Internet Explorer


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/4/2019  12:42 AM             12 passwords.bak.txt
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-Content "C:\Program Files (x86)\Internet Explorer\passwords.bak.txt"
```

Question #11

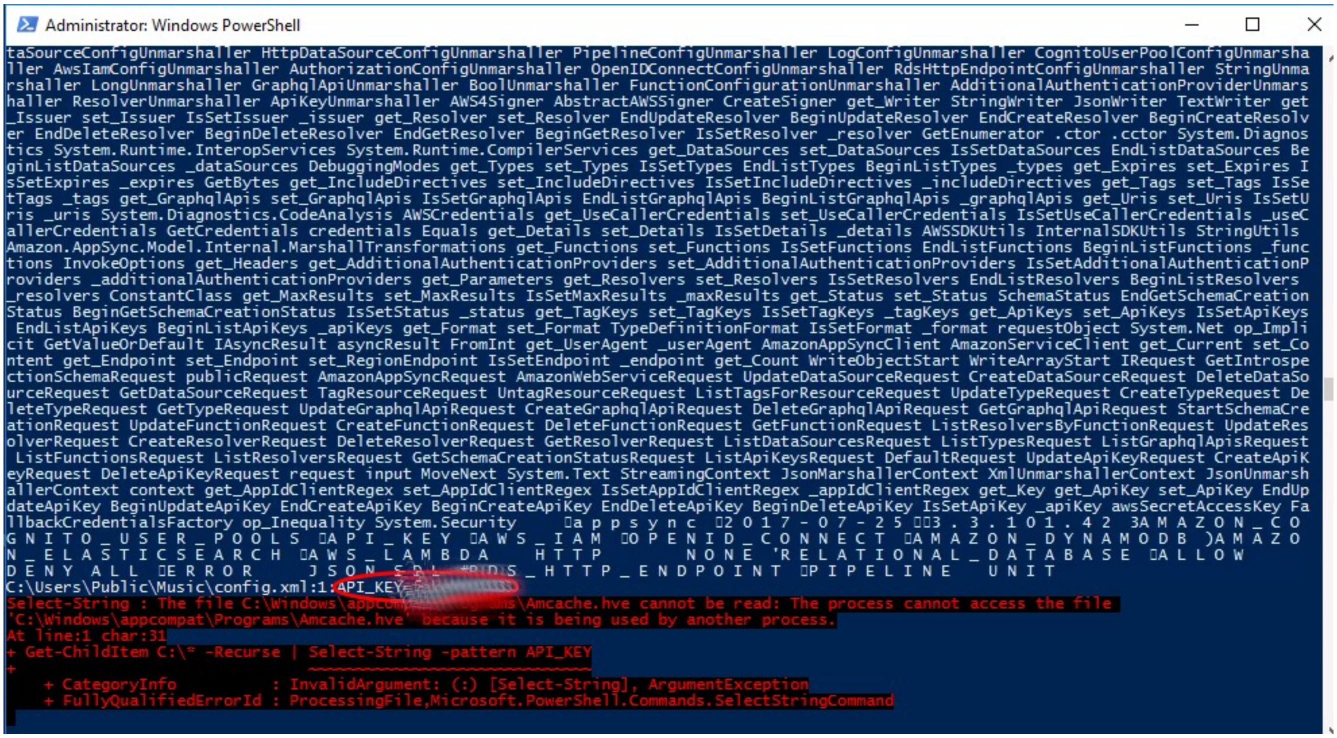
```
Get-ChildItem C:\* -Recurse | Select-String -pattern API_KEY
```



```
PS C:\Users\Administrator> Get-ChildItem C:\* -Recurse | Select-String -pattern API_KEY
_
```

Then after a whole mess of gobbily goo pops out.

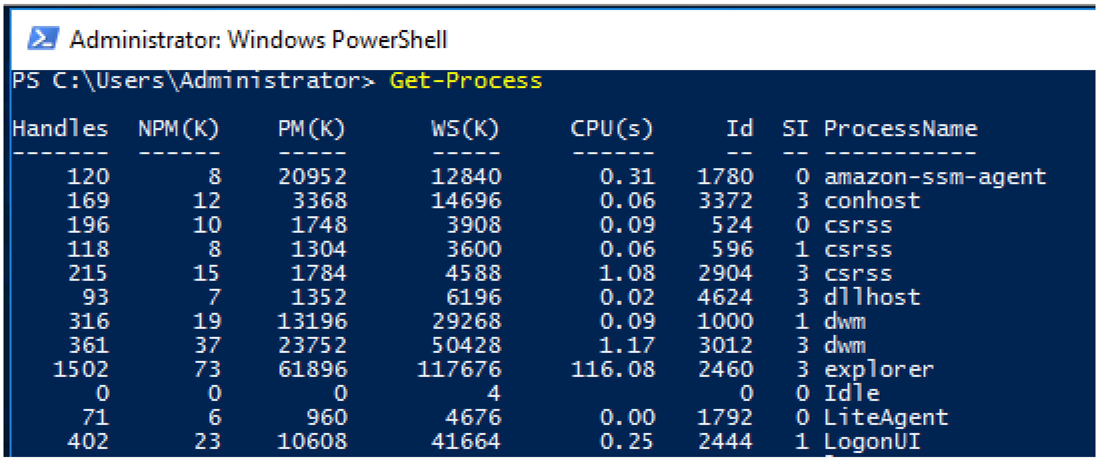
I had to move the results up and down using the sidebar because the API_KEY= was blank lol. Then it magically appeared.



```
taSourceConfigUnmarshaller HttpDataSourceConfigUnmarshaller PipelineConfigUnmarshaller LogConfigUnmarshaller CognitoUserPoolConfigUnmarsha
ller AwsIamConfigUnmarshaller AuthorizationConfigUnmarshaller OpenIDConnectConfigUnmarshaller RdsHttpEndpointConfigUnmarshaller StringUnma
rshaller LongUnmarshaller GraphqlApiUnmarshaller BoolUnmarshaller FunctionConfigurationUnmarshaller AdditionalAuthenticationProviderUnmars
haller ResolverUnmarshaller ApiKeyUnmarshaller AWS4Signer AbstractAWSSigner CreateSigner get_Writer StringWriter JsonWriter TextWriter get
_Issuer set_Issuer IsSetIssuer _issuer get_Resolver set_Resolver EndUpdateResolver BeginUpdateResolver EndCreateResolver BeginCreateResolv
er EndDeleteResolver BeginDeleteResolver EndGetResolver BeginGetResolver IsSetResolver _resolver GetEnumerator .ctor .cctor System.Diagnos
tics System.Runtime.InteropServices System.Runtime.CompilerServices get_DataSources set_DataSources IsSetDataSources EndListDataSources Be
ginListDataSources _dataSources DebuggingModes get_Types set_Types IsSetTypes EndListTypes BeginListTypes _types get_Expires set_Expires I
sSetExpires _expires GetBytes get_IncludeDirectives set_IncludeDirectives IsSetIncludeDirectives _includeDirectives get_Tags set_Tags IsSe
tTags _tags get_GraphqlApis set_GraphqlApis IsSetGraphqlApis EndListGraphqlApis BeginListGraphqlApis _graphqlApis get_Uris set_Uris IsSetU
ris _uris System.Diagnostics.CodeAnalysis AWSCredentials get_UseCallerCredentials set_UseCallerCredentials IsSetUseCallerCredentials _useC
allerCredentials GetCredentials credentials Equals get_Details set_Details IsSetDetails _details AWSSDKUtils InternalSDKUtils StringUtils
Amazon.AppSync.Model.Internal.MarshallTransformations get_Functions set_Functions IsSetFunctions EndListFunctions BeginListFunctions _func
tions InvokeOptions get_Headers get_AdditionalAuthenticationProviders set_AdditionalAuthenticationProviders IsSetAdditionalAuthenticationP
roviders _additionalAuthenticationProviders get_Parameters get_Resolvers set_Resolvers IsSetResolvers EndListResolvers BeginListResolvers
_resolvers ConstantClass get_MaxResults set_MaxResults IsSetMaxResults _maxResults get_Status set_Status SchemaStatus EndGetSchemaCreation
Status BeginGetSchemaCreationStatus IsSetStatus _status get_TagKeys set_TagKeys IsSetTagKeys _tagKeys get_ApiKeys set_ApiKeys IsSetApiKeys
 EndListApiKeys BeginListApiKeys _apiKeys get_Format set_Format TypeDefinitionFormat IsSetFormat _format requestObject System.Net op_Impli
cit GetValueOrDefault IAsyncResult asyncResult FromInt get_UserAgent _userAgent AmazonAppSyncClient AmazonServiceClient get_Current set_Co
ntent get_Endpoint set_Endpoint set_RegionEndpoint IsSetEndpoint _endpoint get_Count WriteObjectStart WriteArrayStart IRequest GetIntrospe
ctionSchemaRequest publicRequest AmazonAppSyncRequest AmazonWebServiceRequest UpdateDataSourceRequest CreateDataSourceRequest DeleteDataSo
urceRequest GetDataSourceRequest TagResourceRequest UntagResourceRequest ListTagsForResourceRequest UpdateTypeRequest CreateTypeRequest De
leteTypeRequest GetTypeRequest UpdateGraphqlApiRequest CreateGraphqlApiRequest DeleteGraphqlApiRequest GetGraphqlApiRequest StartSchemaCre
ationRequest UpdateFunctionRequest CreateFunctionRequest DeleteFunctionRequest GetFunctionRequest ListResolversByFunctionRequest UpdateRes
olverRequest CreateResolverRequest DeleteResolverRequest GetResolverRequest ListDataSourcesRequest ListTypesRequest ListGraphqlApisRequest
 ListFunctionsRequest ListResolversRequest GetSchemaCreationStatusRequest ListApiKeysRequest DefaultRequest UpdateApiKeyRequest CreateApiK
eyRequest DeleteApiKeyRequest request input MoveNext System.Text StreamingContext JsonMarshallerContext XmlUnmarshallerContext JsonUnmarsh
allerContext context get_AppIdClientRegex set_AppIdClientRegex IsSetAppIdClientRegex _appIdClientRegex get_Key get_ApiKey set_ApiKey EndUp
dateApiKey BeginUpdateApiKey EndCreateApiKey BeginCreateApiKey EndDeleteApiKey BeginDeleteApiKey IsSetApiKey _apiKey awsSecretAccessKey Fa
llbackCredentialsFactory op_Inequality System.Security    a p p s y n c  2 0 1 7 - 0 7 - 2 5 3 . 3 . 1 0 1 . 4 2  3A M A Z O N _ C O
G N I T O _ U S E R _ P O O L S  A P I _ K E Y  A W S _ I A M  O P E N I D _ C O N N E C T  A M A Z O N _ D Y N A M O D B  )A M A Z O
N _ E L A S T I C S E A R C H  A W S _ L A M B D A    H T T P       N O N E  'R E L A T I O N A L _ D A T A B A S E  A L L O W
D E N Y  A L L  E R R O R     J S O N                S _ H T T P _ E N D P O I N T  P I P E L I N E   U N I T
C:\Users\Public\Music\config.xml:1:API_KEY=[redacted]
Select-String : The file C:\Windows\appcom           ams\Amcache.hve cannot be read: The process cannot access the file
'C:\Windows\appcompat\Programs\Amcache.hve' because it is being used by another process.
At line:1 char:31
+ Get-ChildItem C:\* -Recurse | Select-String -pattern API_KEY
+                               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Select-String], ArgumentException
    + FullyQualifiedErrorId : ProcessingFile,Microsoft.PowerShell.Commands.SelectStringCommand
```

Question #12

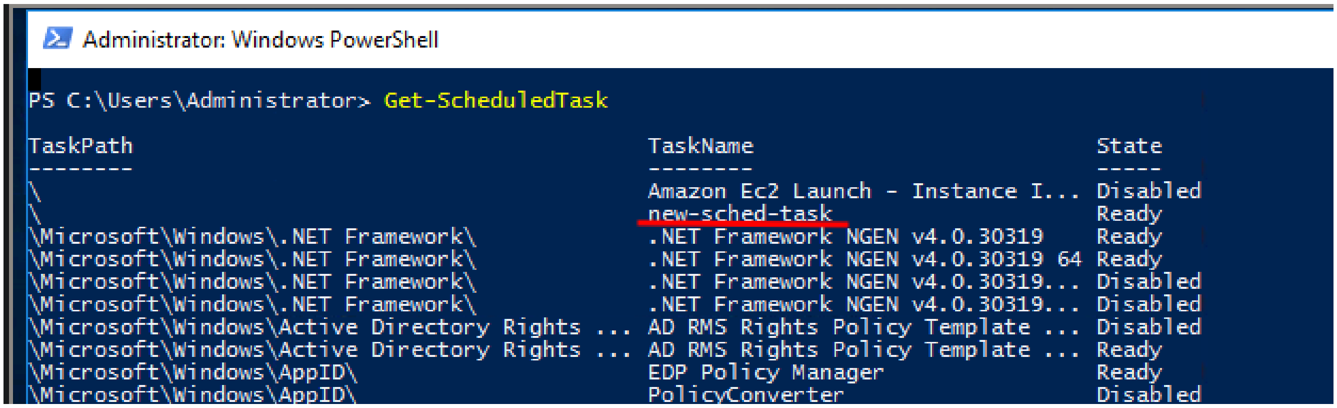
Get-Process



```
PS C:\Users\Administrator> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    120       8    20952      12840       0.31   1780   0 amazon-ssm-agent
    169      12     3368      14696       0.06   3372   3 conhost
    196      10     1748       3908       0.09    524   0 csrss
    118       8     1304       3600       0.06    596   1 csrss
    215      15     1784       4588       1.08   2904   3 csrss
     93       7     1352       6196       0.02   4624   3 dllhost
    316      19    13196      29268       0.09   1000   1 dwm
    361      37    23752      50428       1.17   3012   3 dwm
   1502      73    61896     117676     116.08   2460   3 explorer
      0       0        0          4                 0   0 Idle
     71       6      960       4676       0.00   1792   0 LiteAgent
    402      23    10608      41664       0.25   2444   1 LogonUI
```

Question #13

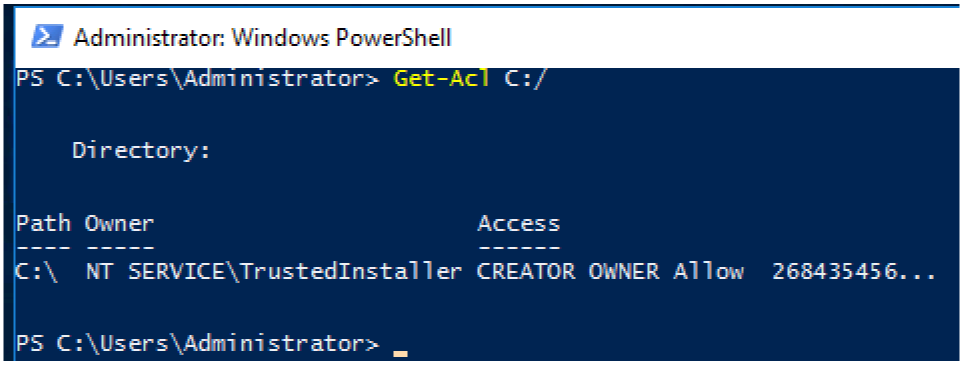
Get-ScheduleTask



```
PS C:\Users\Administrator> Get-ScheduledTask

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\                                              Amazon Ec2 Launch - Instance I... Disabled
\                                              new-sched-task                    Ready
\Microsoft\Windows\.NET Framework\             .NET Framework NGEN v4.0.30319    Ready
\Microsoft\Windows\.NET Framework\             .NET Framework NGEN v4.0.30319 64 Ready
\Microsoft\Windows\.NET Framework\             .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\.NET Framework\             .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Ready
\Microsoft\Windows\AppID\                      EDP Policy Manager                Ready
\Microsoft\Windows\AppID\                      PolicyConverter                   Disabled
```

Question #14

Get-Acl c:/



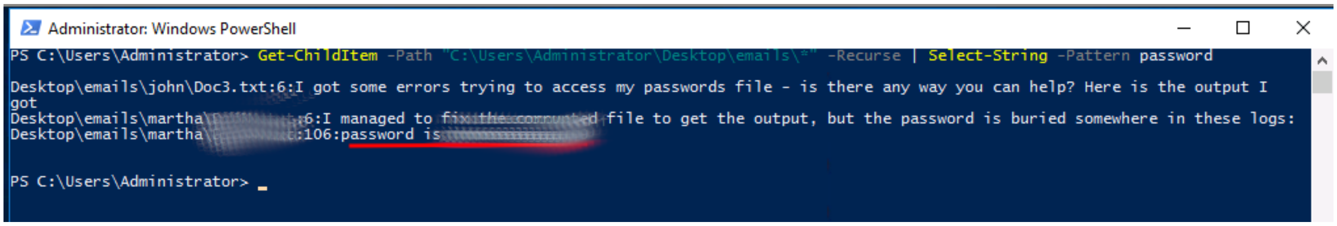
```
PS C:\Users\Administrator> Get-Acl C:/


    Directory:


Path Owner                      Access
---- -----                      ------
C:\  NT SERVICE\TrustedInstaller CREATOR OWNER Allow  268435456...


PS C:\Users\Administrator> _
```

Task 5: Basic Scripting Challenge

Question #1

So, without writing a script you can run this command:

Get-ChildItem -Path "C:\Users\Administrator\Desktop\emails\*" -Recurse | Select-String -Pattern password

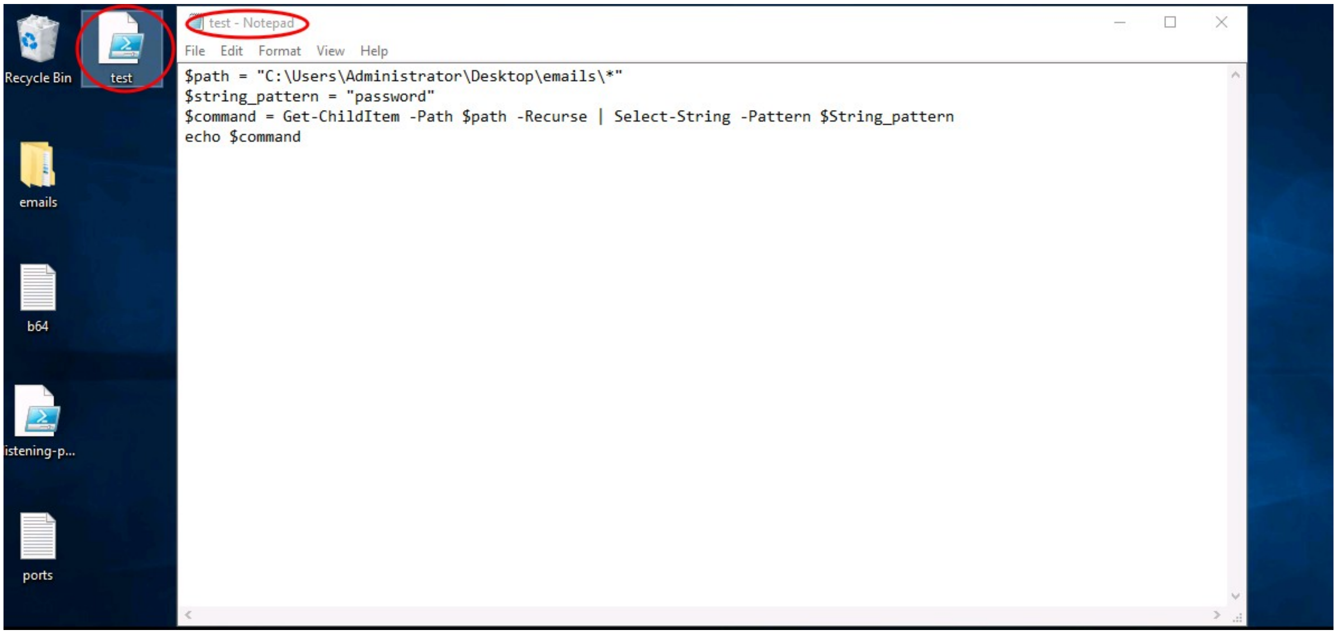


```
PS C:\Users\Administrator> Get-ChildItem -Path "C:\Users\Administrator\Desktop\emails\*" -Recurse | Select-String -Pattern password

Desktop\emails\john\Doc3.txt:6:I got some errors trying to access my passwords file - is there any way you can help? Here is the output I
got
Desktop\emails\martha\[redacted]:6:I managed to [redacted] file to get the output, but the password is buried somewhere in these logs:
Desktop\emails\martha\[redacted]:106:password is [redacted]


PS C:\Users\Administrator> _
```

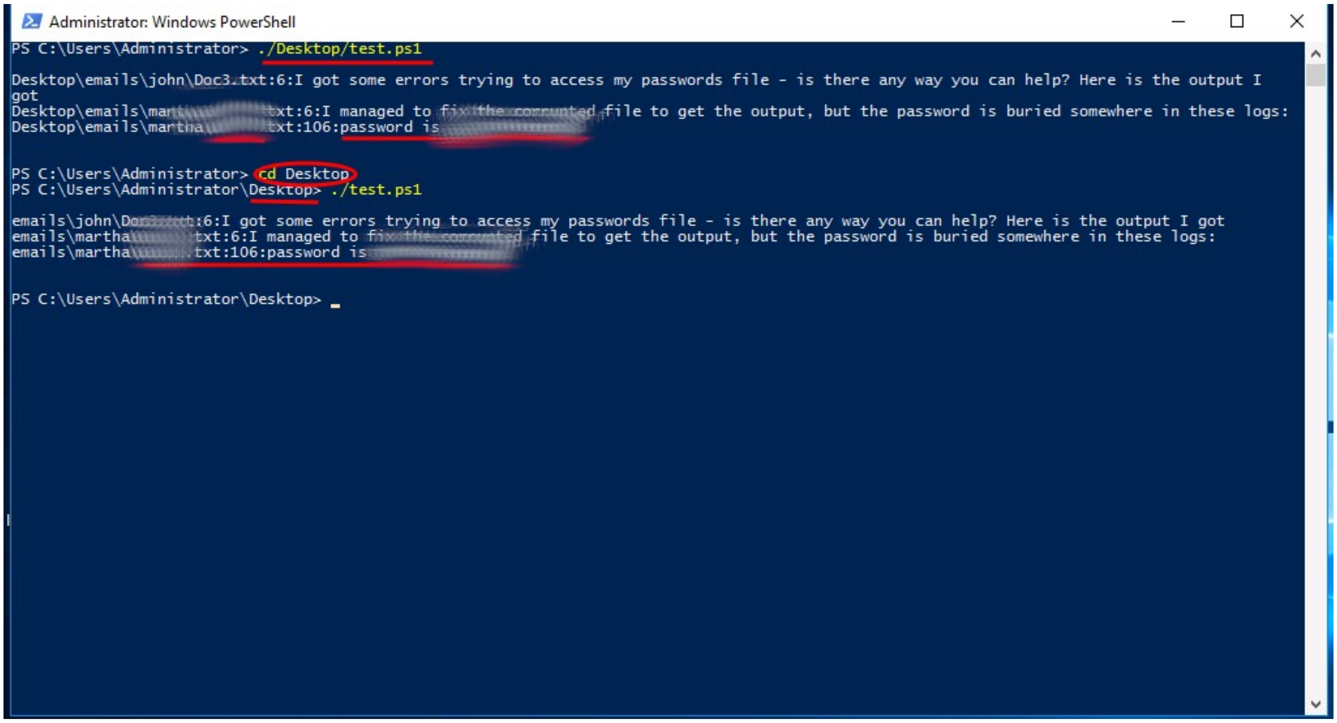
Now, you basically are taking that command and breaking it into one line chunks that powershell will execute one line at a time.

You can open a text editor and put the lines in there and then call the file whatever you want with the extension .ps1   that is a one not the letter l. Then you would type ./yourfile.ps1 and presto !

In this example, the file was saved to the Desktop and named test.ps1.
Then ran the command ./Desktop/test.ps1
If we switched directories to the Desktop then you would just run ./test.ps1   but you have to include the file path if you are not in the same directory as your file.



```
$path = "C:\Users\Administrator\Desktop\emails\*"
$string_pattern = "password"
$command = Get-ChildItem -Path $path -Recurse | Select-String -Pattern $String_pattern
echo $command
```

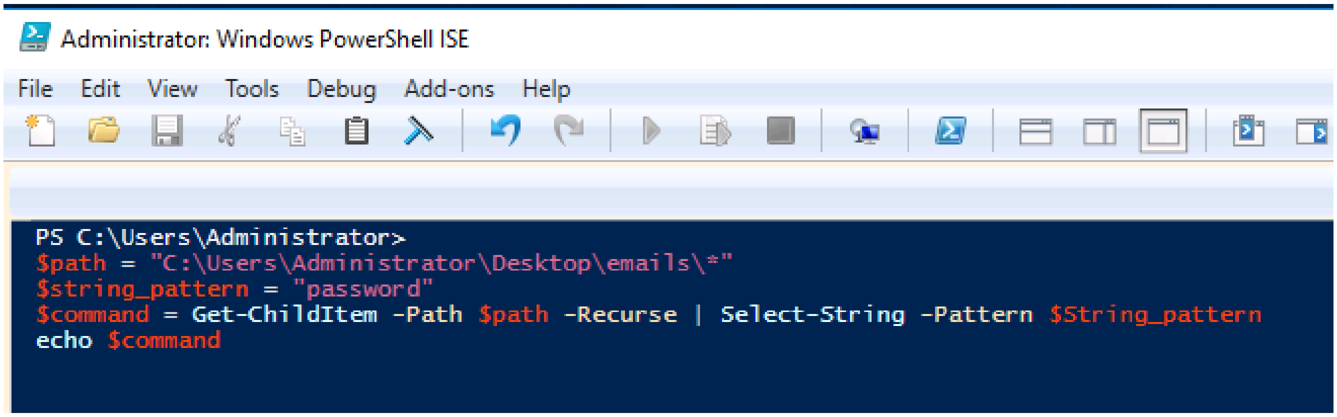


```
PS C:\Users\Administrator> ./Desktop/test.ps1

Desktop\emails\john\Doc3.txt:6:I got some errors trying to access my passwords file - is there any way you can help? Here is the output I
got
Desktop\emails\mar[redacted]txt:6:I managed to [redacted] file to get the output, but the password is buried somewhere in these logs:
Desktop\emails\martha[redacted]txt:106:password is [redacted]

PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> ./test.ps1

emails\john\Do[redacted]:6:I got some errors trying to access my passwords file - is there any way you can help? Here is the output I got
emails\martha[redacted]txt:6:I managed to [redacted] file to get the output, but the password is buried somewhere in these logs:
emails\martha[redacted].txt:106:password is [redacted]

PS C:\Users\Administrator\Desktop> _
```

Second option is to use the powershell ISE which is sort of like doing the text editor option but live from the powershell terminal. It’s kind of like a coding IDE where as you type cmdlets it will have pop ups to help you along the way with what options are available.

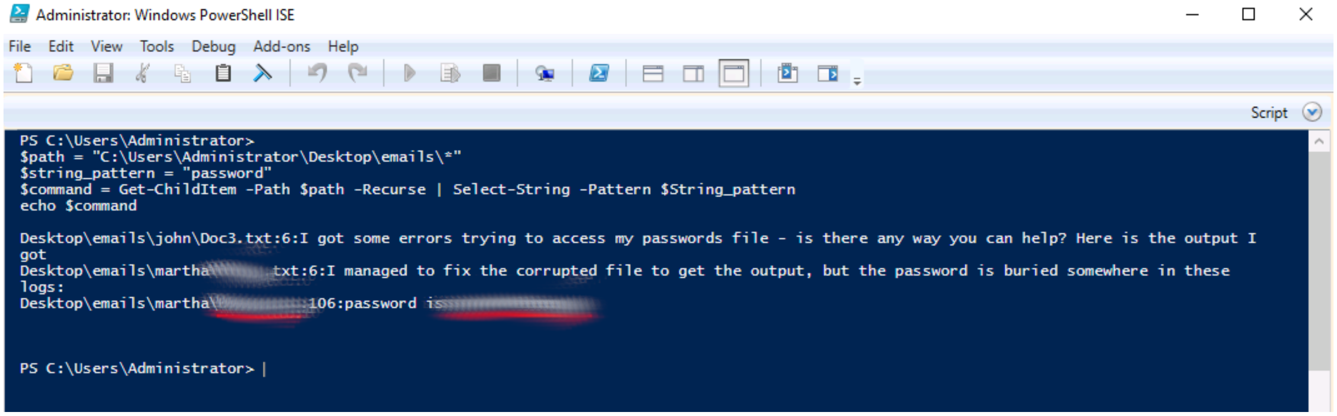
If you want to move down a line in the ISE hold down your shift key and then hit Enter/Return key. If you do not hold down shift you will run the command.

```
$path = "C:\Users\Administrator\Desktop\emails\*"
$string_pattern = "password"
$command = Get-ChildItem -Path $path -Recurse | Select-String -Pattern
$String_pattern

echo $command
```



Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

```
PS C:\Users\Administrator>
$path = "C:\Users\Administrator\Desktop\emails\*"
$string_pattern = "password"
$command = Get-ChildItem -Path $path -Recurse | Select-String -Pattern $String_pattern
echo $command
```



Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

```
PS C:\Users\Administrator>
$path = "C:\Users\Administrator\Desktop\emails\*"
$string_pattern = "password"
$command = Get-ChildItem -Path $path -Recurse | Select-String -Pattern $String_pattern
echo $command

Desktop\emails\john\Doc3.txt:6:I got some errors trying to access my passwords file - is there any way you can help? Here is the output I
got
Desktop\emails\martha[redacted]txt:6:I managed to fix the corrupted file to get the output, but the password is buried somewhere in these
logs:
Desktop\emails\martha\[redacted]106:password is[redacted]


PS C:\Users\Administrator> |
```

Question #2

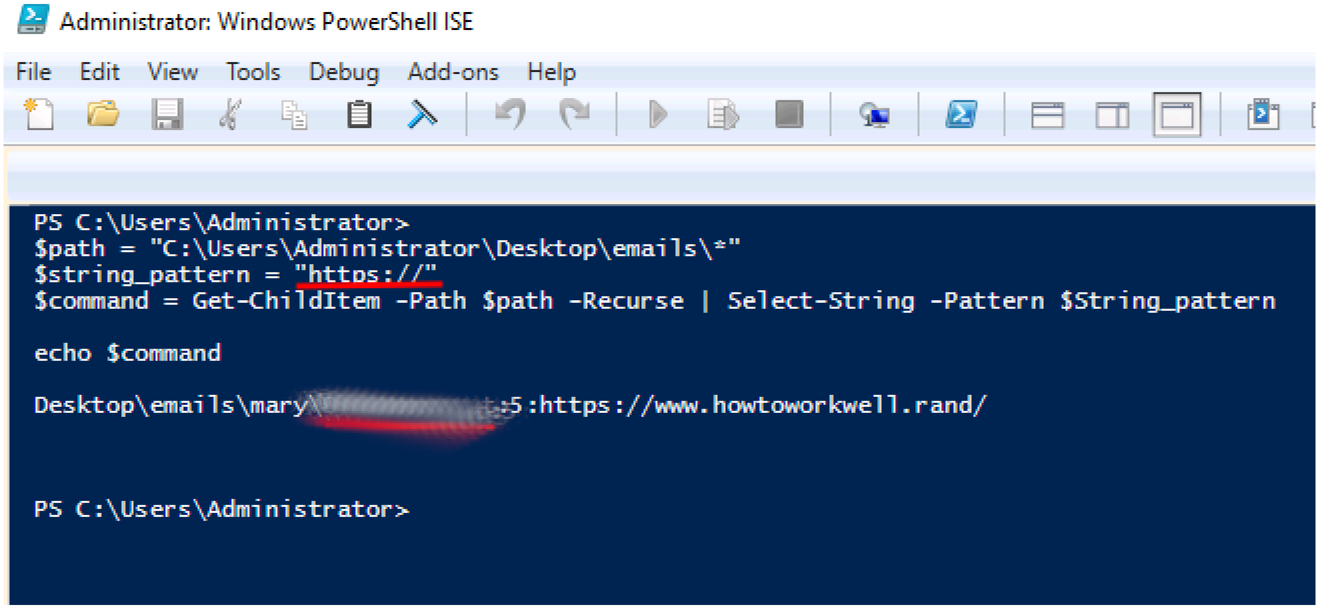
The answer was shown in Question #1

Question #3

Literally, the only thing that changes from the previous script is the “https://”

So, just hit the up arrow on your key board to cycle through previous commands so you don’t have to type it all out again.

```
$path = "C:\Users\Administrator\Desktop\emails\*"

$string_pattern = "https://"
$command = Get-ChildItem -Path $path -Recurse | Select-String -Pattern
$String_pattern

$echo $command
```



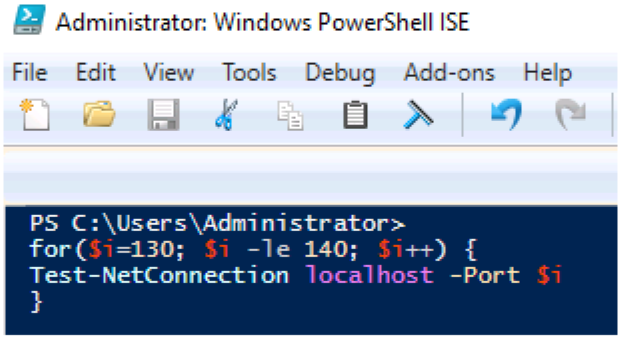
```
PS C:\Users\Administrator>
$path = "C:\Users\Administrator\Desktop\emails\*"
$string_pattern = "https://"
$command = Get-ChildItem -Path $path -Recurse | Select-String -Pattern $String_pattern

echo $command

Desktop\emails\mary\[redacted]5:https://www.howtoworkwell.rand/


PS C:\Users\Administrator>
```

Task 6: Intermediate Scripting

Question #1

So, the idea is to write a for loop like this

```
for($i=130; $i -le 140; $i++){

  Test-NetConnection localhost -Port $i

}
```



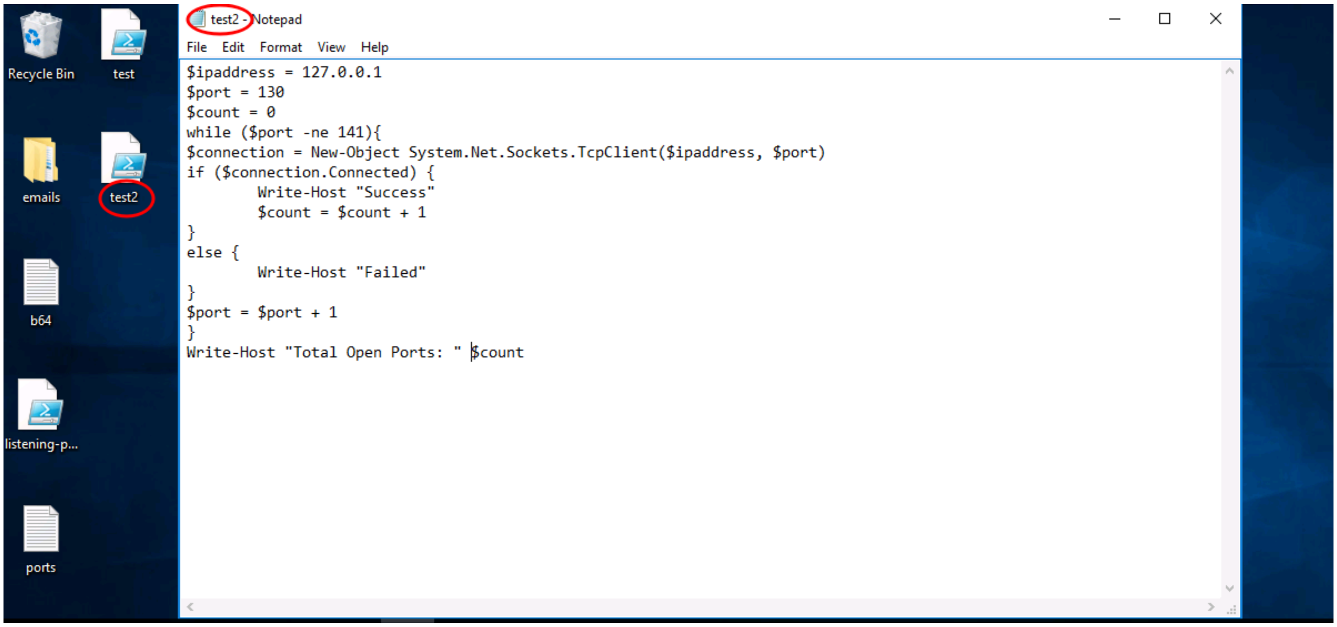
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

```
PS C:\Users\Administrator>
for($i=130; $i -le 140; $i++) {
Test-NetConnection localhost -Port $i
}
```

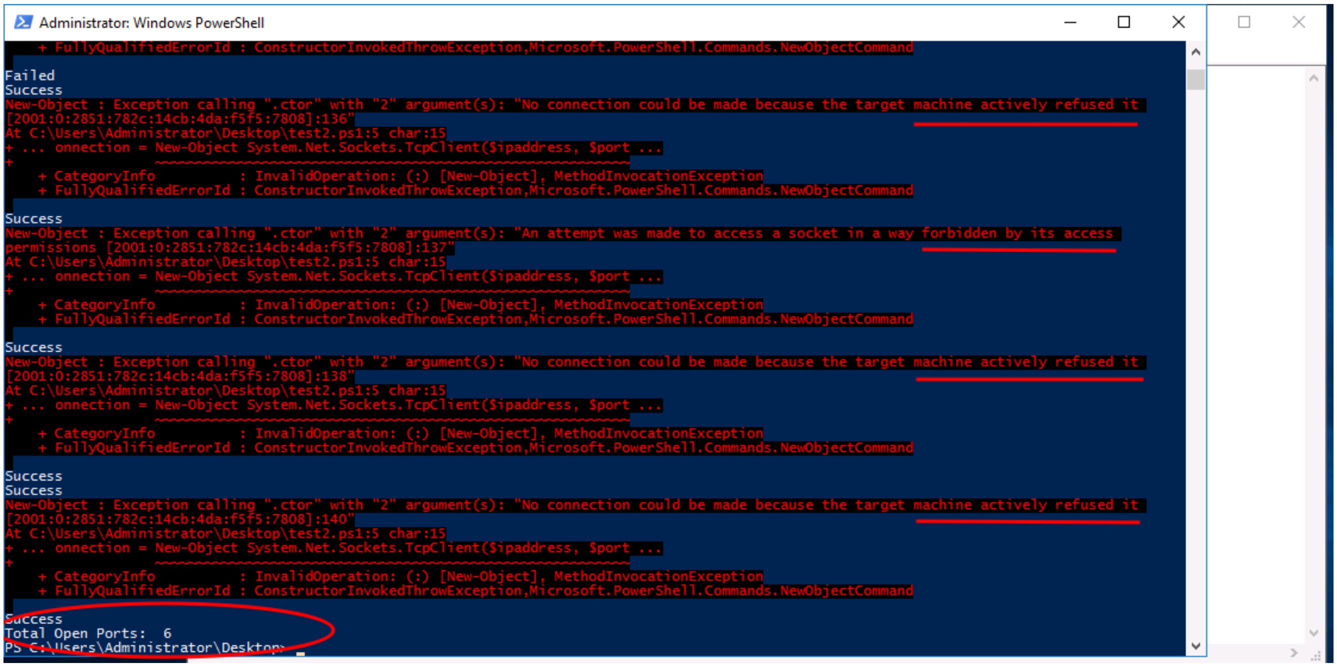
When you do, the result comes back as 1 BUT that is incorrect. The answer is the total number of ports we scanned with this script. Which is incorrect lol. We are supposed to be getting the total open ports from the IPs in the range 130-140.

This script gives you 6 open connections. It looks like something is actively shooting down the connection attempts.

```
$ipaddress = 127.0.0.1

$port = 130
$count = 0
while ($port -ne 141) {
$connection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port)
if ($connection.Connected) {
      Write-Host "Success"
      $count = $count + 1
}
else {
      Write-Host "Failed"
}

$port = $port + 1

}

Write-Host “Total Open Ports: “ $count
```



```
$ipaddress = 127.0.0.1
$port = 130
$count = 0
while ($port -ne 141){
$connection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port)
if ($connection.Connected) {
        Write-Host "Success"
        $count = $count + 1
}
else {
        Write-Host "Failed"
}
$port = $port + 1
}
Write-Host "Total Open Ports: " $count
```



```
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewObjectCommand

Failed
Success
New-Object : Exception calling ".ctor" with "2" argument(s): "No connection could be made because the target machine actively refused it
[2001:0:2851:782c:14cb:4da:f5f5:7808]:136"
At C:\Users\Administrator\Desktop\test2.ps1:5 char:15
+ ... onnection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port ...
+               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [New-Object], MethodInvocationException
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewObjectCommand

Success
New-Object : Exception calling ".ctor" with "2" argument(s): "An attempt was made to access a socket in a way forbidden by its access
permissions [2001:0:2851:782c:14cb:4da:f5f5:7808]:137"
At C:\Users\Administrator\Desktop\test2.ps1:5 char:15
+ ... onnection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port ...
+               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [New-Object], MethodInvocationException
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewObjectCommand

Success
New-Object : Exception calling ".ctor" with "2" argument(s): "No connection could be made because the target machine actively refused it
[2001:0:2851:782c:14cb:4da:f5f5:7808]:138"
At C:\Users\Administrator\Desktop\test2.ps1:5 char:15
+ ... onnection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port ...
+               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [New-Object], MethodInvocationException
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewObjectCommand

Success
Success
New-Object : Exception calling ".ctor" with "2" argument(s): "No connection could be made because the target machine actively refused it
[2001:0:2851:782c:14cb:4da:f5f5:7808]:140"
At C:\Users\Administrator\Desktop\test2.ps1:5 char:15
+ ... onnection = New-Object System.Net.Sockets.TcpClient($ipaddress, $port ...
+               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [New-Object], MethodInvocationException
    + FullyQualifiedErrorId : ConstructorInvokedThrowException,Microsoft.PowerShell.Commands.NewObjectCommand

Success
Total Open Ports:  6
PS C:\Users\Administrator\Desktop> _
```

Play around and see if you can get more open ports.

Happy Hacking !!