Mark Seliternikov
TryHackMe - Hacking With PowerShell [Easy]

In this lab I practiced using PowerShell. This will be very useful for enumeration in windows if the need arises. I am given a machine and in this scenario I am already in and I just need to collect information.

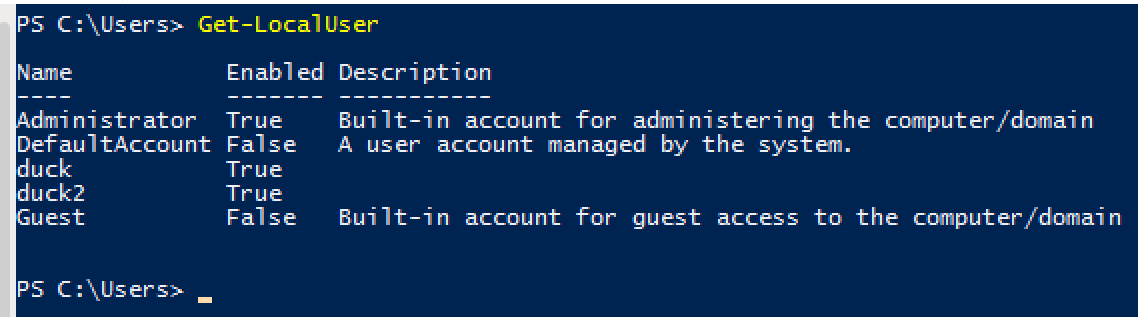
Cheat Sheet:
https://gist.github.com/pcgeek86/336e08d1a09e3dd1a8f0a30a9fe61c8a

Useful commands to know in general:

- **Get-Help** (-detailed, -example)
- **Get-Command**
- **Get-ChildItem**
- **Get-Member**
- **Where-Object**
- **Sort-Object**
- **Measure-Object** (count lines, words, etc...)
- **Get-FileHash** (Get hash with various algorithms)
- **Invoke-WebRequest** (like curl in linux)
- **Get-LocalUser**
- **wmic** (useful to get info on users)
- **Get-Process**
- **Get-LocalGroup**
- **Get-NetIPAddress**
- **Get-NetTCPConnection**
- **Select-String -Pattern <string>** (equivalent to “grep”)
- **Get-HotFix** (get patches info)
- **Get-acl** (see owner of files/ directories)
- **Test-NetConnectio**

Enumeration

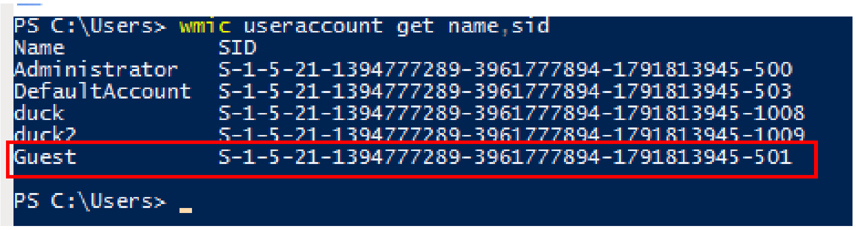
How many users are on the machine?:



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

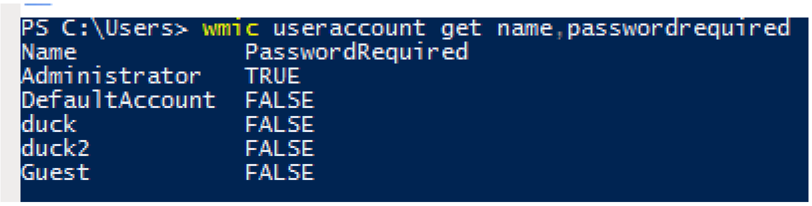
- Answer: 5 (can use “| Measure-Object -Line”)

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



```
PS C:\Users> wmic useraccount get name,sid
Name            SID
Administrator   S-1-5-21-1394777289-3961777894-1791813945-500
DefaultAccount  S-1-5-21-1394777289-3961777894-1791813945-503
duck            S-1-5-21-1394777289-3961777894-1791813945-1008
duck2           S-1-5-21-1394777289-3961777894-1791813945-1009
Guest           S-1-5-21-1394777289-3961777894-1791813945-501

PS C:\Users> _
```

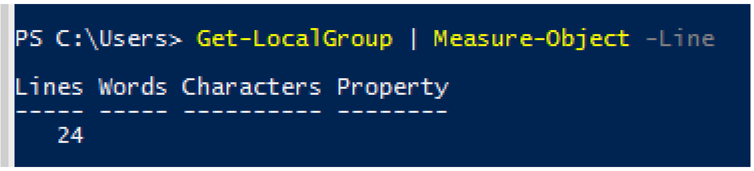
How many users have their password required values set to False?



```
PS C:\Users> wmic useraccount get name,passwordrequired
Name            PasswordRequired
Administrator   TRUE
DefaultAccount  FALSE
duck            FALSE
duck2           FALSE
Guest           FALSE
```

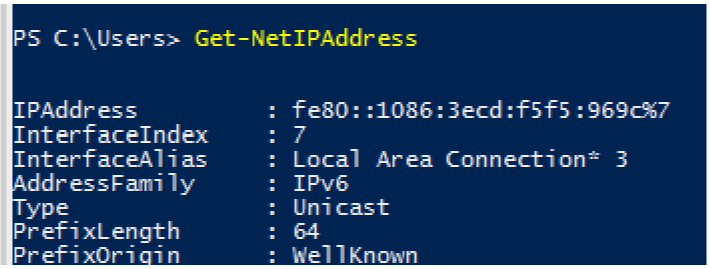
- Answer: 4 (can use "| Measure-Object -Line")

How many local groups exist?



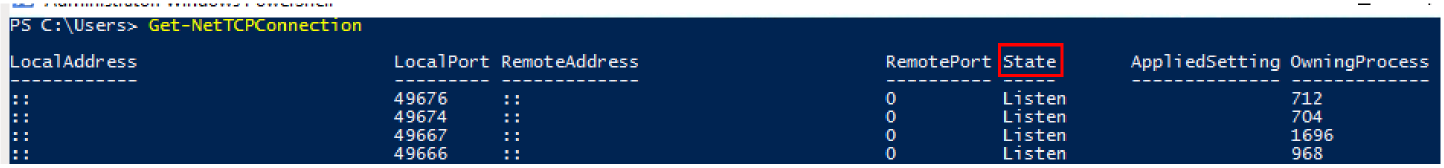
```
PS C:\Users> Get-LocalGroup | Measure-Object -Line

Lines Words Characters Property
----- ----- ---------- --------
   24
```

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

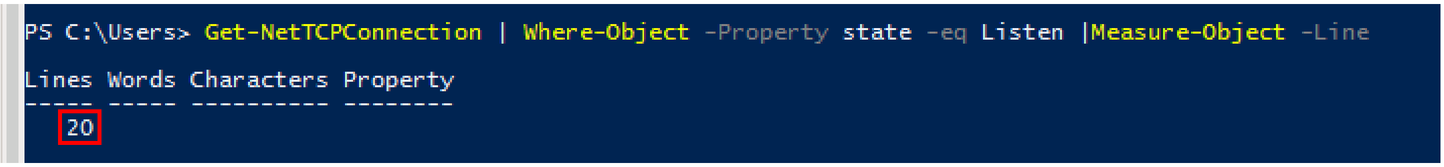


```
PS C:\Users> Get-NetIPAddress


IPAddress         : fe80::1086:3ecd:f5f5:969c%7
InterfaceIndex    : 7
InterfaceAlias    : Local Area Connection* 3
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
```

How many ports are listed as listening?

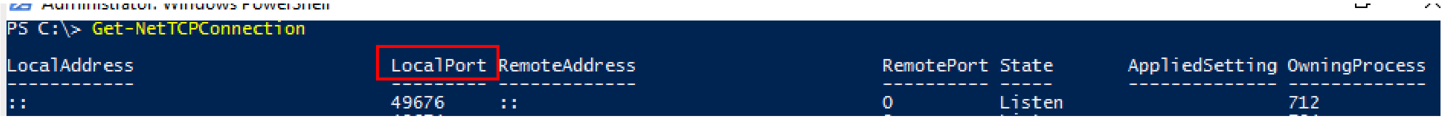


```
PS C:\Users> Get-NetTCPConnection

LocalAddress                        LocalPort RemoteAddress                        RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                        ---------- -----       -------------- -------------
::                                  49676     ::                                   0          Listen                     712
::                                  49674     ::                                   0          Listen                     704
::                                  49667     ::                                   0          Listen                     1696
::                                  49666     ::                                   0          Listen                     968
```

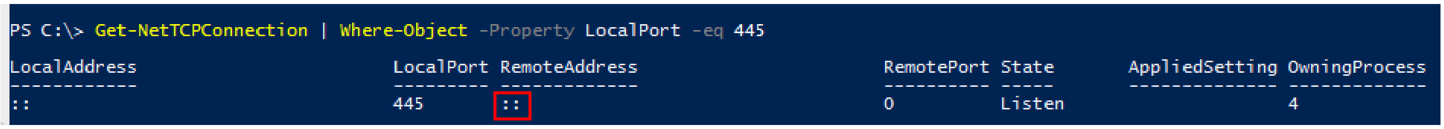


```
PS C:\Users> Get-NetTCPConnection | Where-Object -Property state -eq Listen |Measure-Object -Line

Lines Words Characters Property
----- ----- ---------- --------
   20
```

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

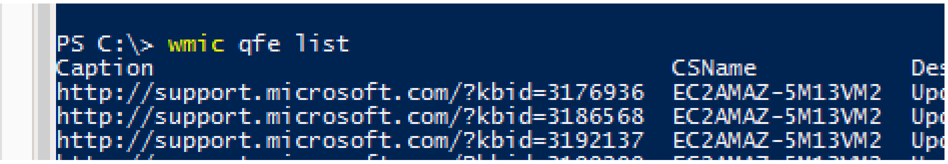


```
PS C:\> Get-NetTCPConnection

LocalAddress                        LocalPort RemoteAddress                        RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                        ---------- -----       -------------- -------------
::                                  49676     ::                                   0          Listen                     712
```

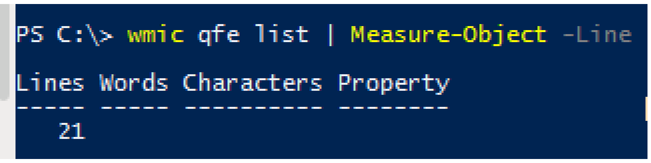


```
PS C:\> Get-NetTCPConnection | Where-Object -Property LocalPort -eq 445

LocalAddress                        LocalPort RemoteAddress                        RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                        ---------- -----       -------------- -------------
::                                  445       ::                                   0          Listen                     4
```

How many patches have been applied?



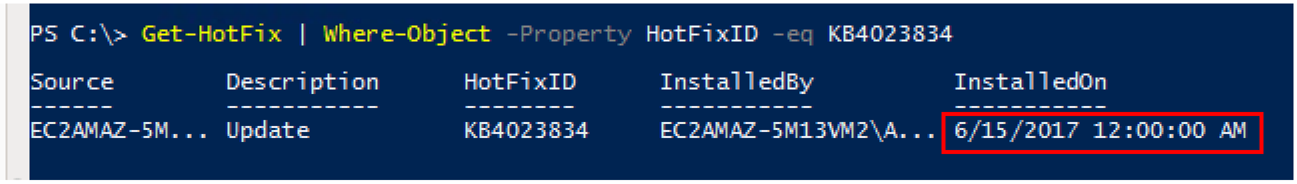
```
PS C:\> wmic qfe list
Caption                                    CSName           Des
http://support.microsoft.com/?kbid=3176936  EC2AMAZ-5M13VM2  Upd
http://support.microsoft.com/?kbid=3186568  EC2AMAZ-5M13VM2  Upd
http://support.microsoft.com/?kbid=3192137  EC2AMAZ-5M13VM2  Upd
```



```
PS C:\> wmic qfe list | Measure-Object -Line

Lines Words Characters Property
----- ----- ---------- --------
   21
```

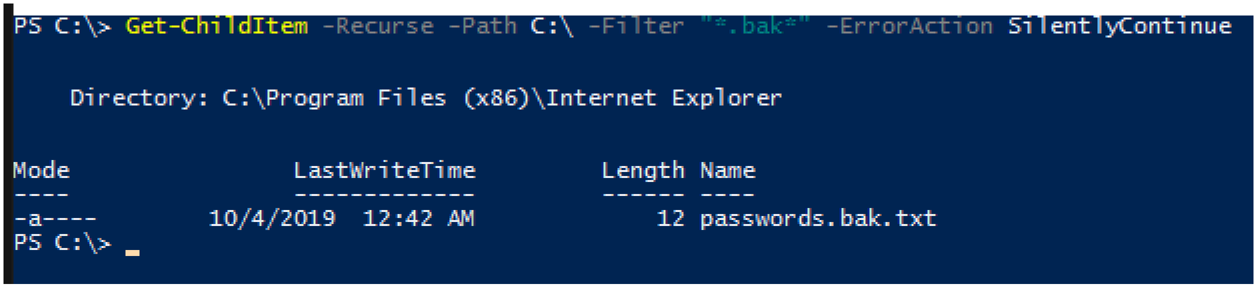
- Answer: 20, The reason is because it counts the first line also (Caption, CSName...)
- Apparently there's an easier method using Get-HotFix.

When was the patch with id KB4023834 installed?

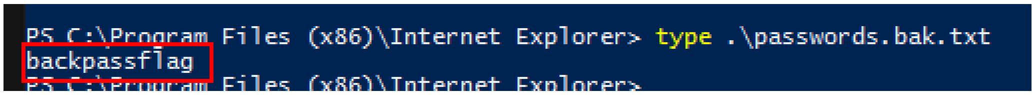


```
PS C:\> Get-HotFix | Where-Object -Property HotFixID -eq KB4023834

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

Find the contents of a backup file:
For this, a little research is needed because I didn't know really makes a file a backup file.
So I found this: https://en.wikipedia.org/wiki/Bak_file. Basically, a file with ".bak" extension.



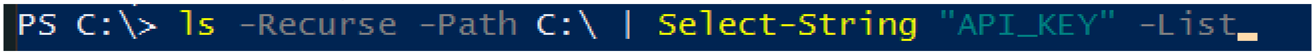
```
PS C:\> Get-ChildItem -Recurse -Path C:\ -Filter "*.bak*" -ErrorAction SilentlyContinue


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


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/4/2019  12:42 AM             12 passwords.bak.txt
PS C:\> _
```



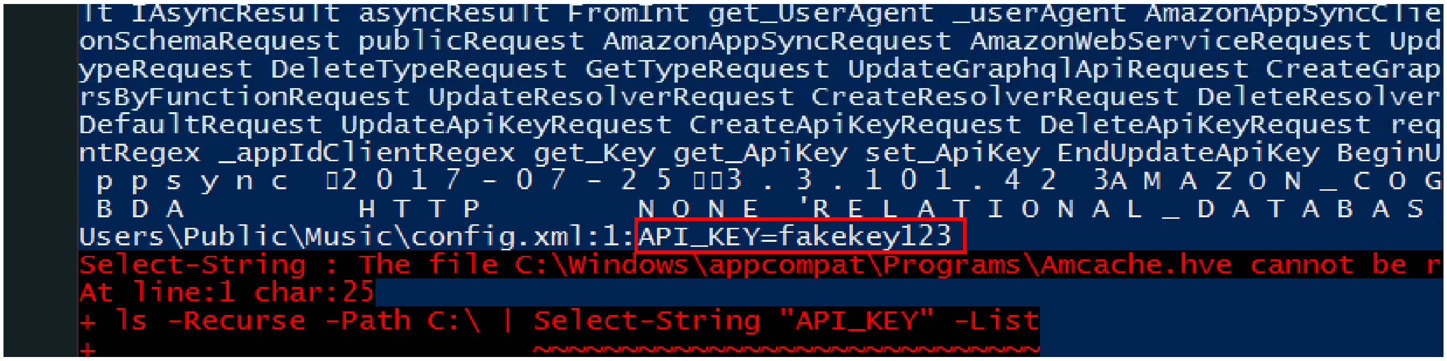
```
PS C:\Program Files (x86)\Internet Explorer> type .\passwords.bak.txt
backpassflag
PS C:\Program Files (x86)\Internet Explorer>
```

We found a flag :)

Search for all files containing API_KEY:
You can do this with the "grep" equivalent "select-string"

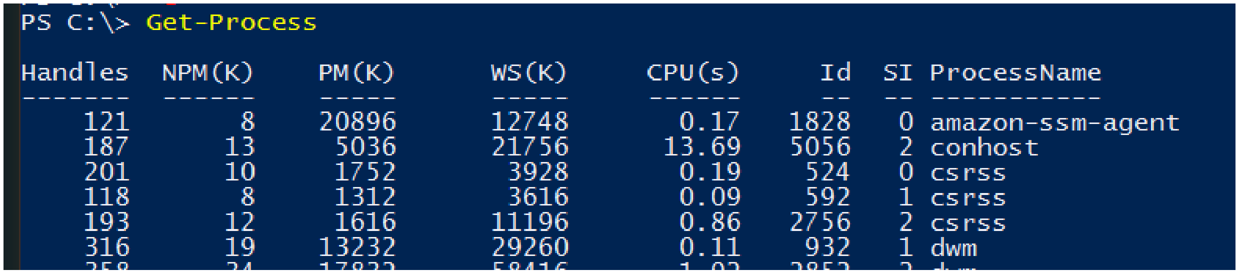


```
PS C:\> ls -Recurse -Path C:\ | Select-String "API_KEY" -List_
```



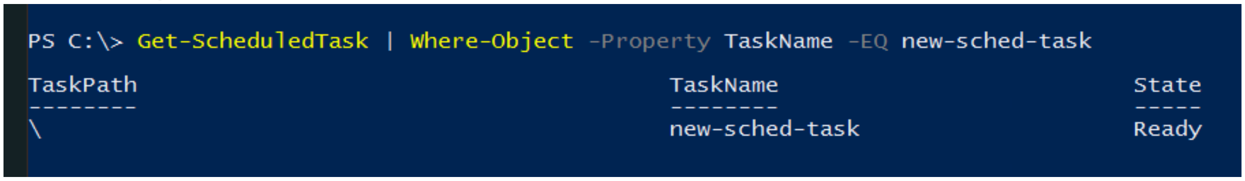
```
lt IAsyncResult asyncResult FromInt get_UserAgent _userAgent AmazonAppSyncClie
onSchemaRequest publicRequest AmazonAppSyncRequest AmazonWebServiceRequest Upd
ypeRequest DeleteTypeRequest GetTypeRequest UpdateGraphqlApiRequest CreateGrap
rsByFunctionRequest UpdateResolverRequest CreateResolverRequest DeleteResolver
DefaultRequest UpdateApiKeyRequest CreateApiKeyRequest DeleteApiKeyRequest req
ntRegex _appIdClientRegex get_Key get_ApiKey set_ApiKey EndUpdateApiKey BeginU
 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
 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
Users\Public\Music\config.xml:1:API_KEY=fakekey123
Select-String : The file C:\Windows\appcompat\Programs\Amcache.hve cannot be r
At line:1 char:25
+ ls -Recurse -Path C:\ | Select-String "API_KEY" -List
+                         ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

List all running processes:



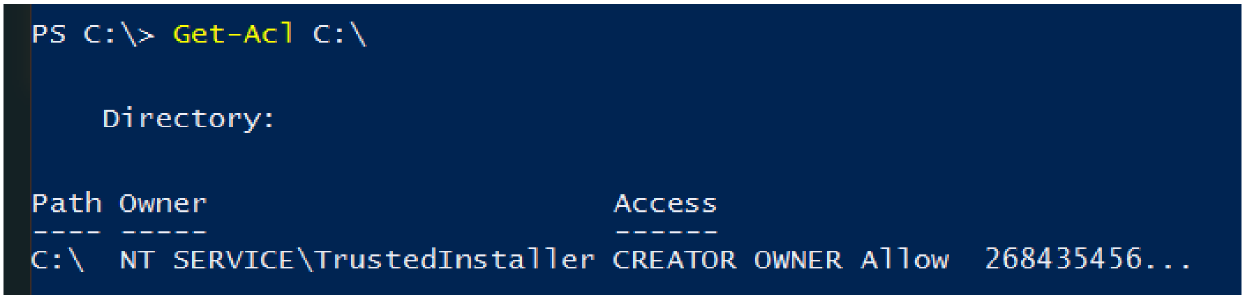
```
PS C:\> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    121       8    20896      12748       0.17   1828   0 amazon-ssm-agent
    187      13     5036      21756      13.69   5056   2 conhost
    201      10     1752       3928       0.19    524   0 csrss
    118       8     1312       3616       0.09    592   1 csrss
    193      12     1616      11196       0.86   2756   2 csrss
    316      19    13232      29260       0.11    932   1 dwm
```

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



```
PS C:\> Get-ScheduledTask | Where-Object -Property TaskName -EQ new-sched-task

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\                                              new-sched-task                    Ready
```

Who is the owner of C:\ ?

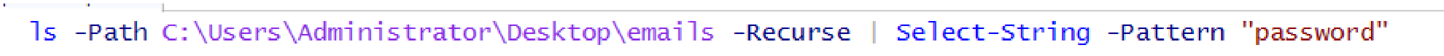


```
PS C:\> Get-Acl C:\


    Directory:


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

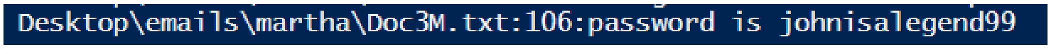
Basic Scripting Challenge

- # Scripting is done with PowerShell ISE (powershell text editor).

What folder contains the password? (in the emails folder on the desktop)
This one is very simple and no script is actually needed, just a combination of 2 commands in a pipeline.



```
ls -Path C:\Users\Administrator\Desktop\emails -Recurse | Select-String -Pattern "password"
```

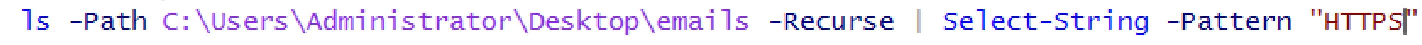


```
Desktop\emails\martha\Doc3M.txt:106:password is johnisalegend99
```

What is the password? (using the same script as in the previous question)

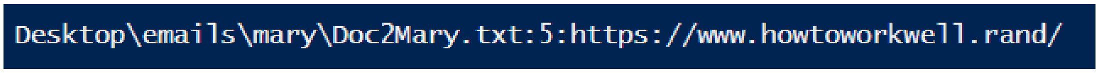
- Answer: johnisalegend99

What files contain an HTTPS link?
This one is very simple as well…



```
ls -Path C:\Users\Administrator\Desktop\emails -Recurse | Select-String -Pattern "HTTPS"
```

Just change the string to “HTTPS”



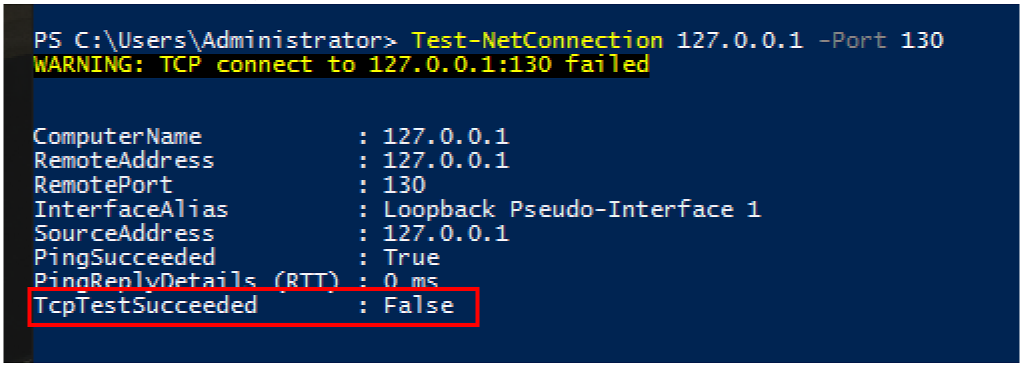
```
Desktop\emails\mary\Doc2Mary.txt:5:https://www.howtoworkwell.rand/
```

Intermediate Scripting

PowerShell port scanner: (On Localhost = 127.0.0.1)

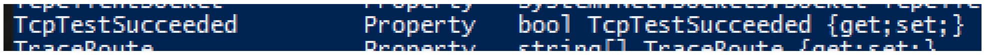
How many open ports did you find between 130 and 140 (inclusive of those two)?

So first I wanted to see how can I connect to a port in PowerShell in general. Apparently there's a handy command for that :)



```
PS C:\Users\Administrator> Test-NetConnection 127.0.0.1 -Port 130
WARNING: TCP connect to 127.0.0.1:130 failed


ComputerName           : 127.0.0.1
RemoteAddress          : 127.0.0.1
RemotePort             : 130
InterfaceAlias         : Loopback Pseudo-Interface 1
SourceAddress          : 127.0.0.1
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

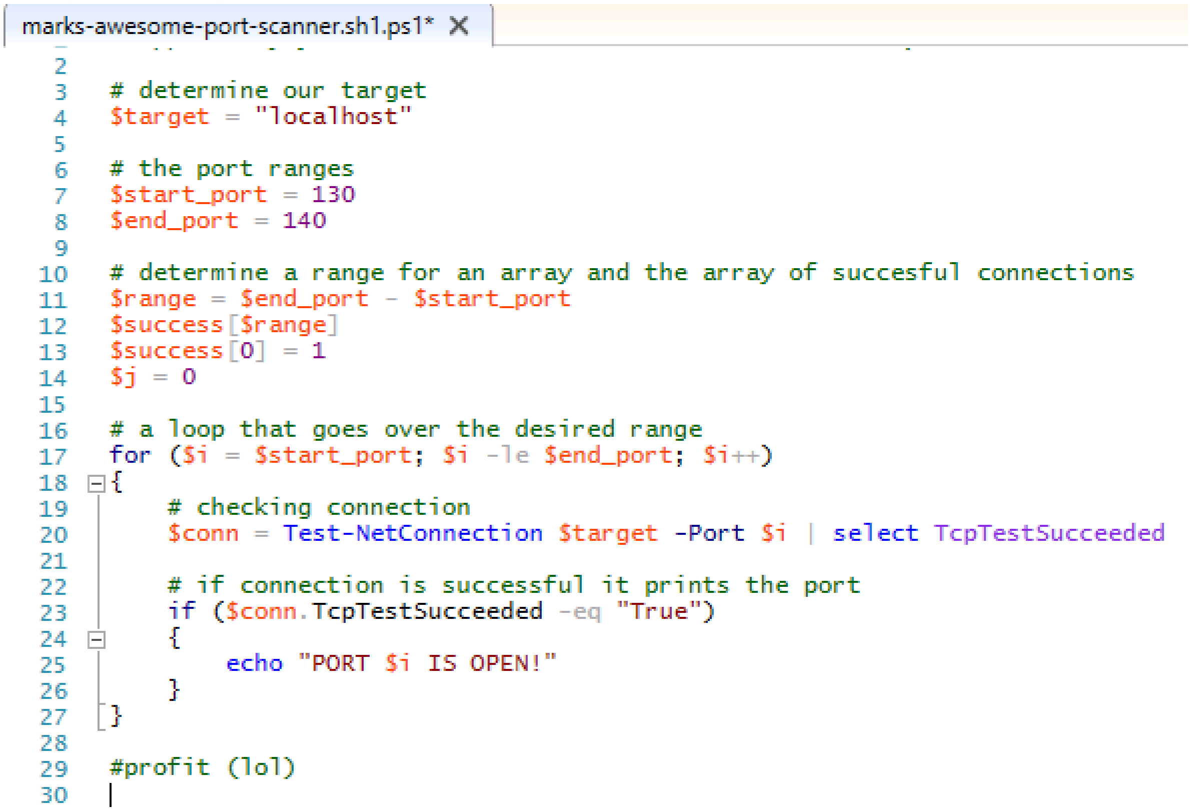
We can see that this command tells me whether the connection was successful or not.
Now I want to discover how can I refer to it, So i'll use Get-Member to check that property.



```
TcpTestSucceeded         Property    bool TcpTestSucceeded {get;set;}
TraceRoute               Property    string[] TraceRoute {get;set;}
```

I can just refer to it with it's name. I need to check whether this value is True or False to each port I try to connect to (130-140).

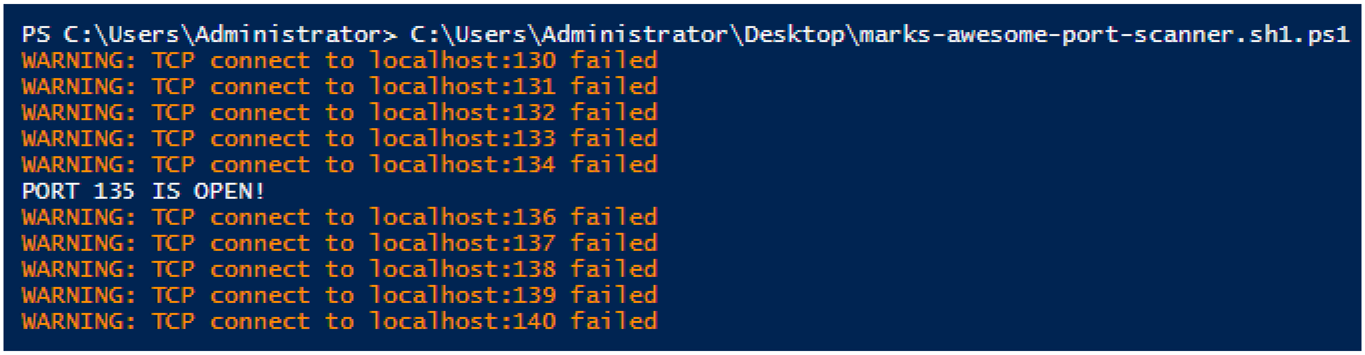
Lets get scripting!



marks-awesome-port-scanner.sh1.ps1*

```

# determine our target
$target = "localhost"

# the port ranges
$start_port = 130
$end_port = 140

# determine a range for an array and the array of succesful connections
$range = $end_port - $start_port
$success[$range]
$success[0] = 1
$j = 0

# a loop that goes over the desired range
for ($i = $start_port; $i -le $end_port; $i++)
{
    # checking connection
    $conn = Test-NetConnection $target -Port $i | select TcpTestSucceeded

    # if connection is successful it prints the port
    if ($conn.TcpTestSucceeded -eq "True")
    {
        echo "PORT $i IS OPEN!"
    }
}

#profit (lol)

```

This is the result! :)



```
PS C:\Users\Administrator> C:\Users\Administrator\Desktop\marks-awesome-port-scanner.sh1.ps1
WARNING: TCP connect to localhost:130 failed
WARNING: TCP connect to localhost:131 failed
WARNING: TCP connect to localhost:132 failed
WARNING: TCP connect to localhost:133 failed
WARNING: TCP connect to localhost:134 failed
PORT 135 IS OPEN!
WARNING: TCP connect to localhost:136 failed
WARNING: TCP connect to localhost:137 failed
WARNING: TCP connect to localhost:138 failed
WARNING: TCP connect to localhost:139 failed
WARNING: TCP connect to localhost:140 failed
```

However, the answer in TryHackMe is 11! Most likely it is a mistake by the creator of the room (Probably miss-clicked 1 again...)