

HACKING WITH POWERSHELL

Counting # of Cmdlets on system with "measure"

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

Count      : 7936
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :
```

Finding a Scheduledtask

```
PS C:\Users\Administrator> Get-Scheduledtask -TaskName new-sched-task

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

Finding all files that contain ".bak" in the the filename. Use of *(wildcards) to detect odd extensions like below:

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

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

Mode                LastWriteTime         Length Name
----                -
----          10/4/2019 12:42 AM             12 passwords.bak.txt
```

Get-Content is like cat cmd in linux:

```
PS C:\Users\Administrator> Get-Content "C:\Program Files (x86)\Internet Explorer\passwords.bak.txt"
backpassflag

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

Get-LocalGroup lists all the groups on the system:

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

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

like grep, this command will search thru all files for the key searchword
"API_KEY"

```
C:\Users\Public\Music\config.xml:1:API_KEY=fakekey123  
Select-String : The file C:\Windows\appcompat\Programs\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  
  
PS C:\Users\Administrator> Get-ChildItem C:\* -Recurse | Select-String -pattern API_KEY
```