WORKING HARD??? YOU DESERVE ARRAYS!

BLAKE REGAN

SENIOR SECURITY ANALYST

FEBRUARY 11TH, 2021

DC CYBER SECURITY PROFESSIONALS

WHOAMI

- Blake Regan (@crash0ver1d3)
  - Father and Husband
  - Started in IT in 2010, formerly worked in Construction Industry
  - Started in Information Security 2014
  - Hockey Fanatic (Fan and Player)
  - Automation enthusiast
  - Serial Learner

EMPLOYMENT AND EDUCATION

- Senior Security Analyst at Wesco Distribution, Inc
- Previously Motorola Solutions, Government and Public Safety: Information Assurance Vetting
- BASc, Information Systems Security
- Certs:
  - GIAC GCWN, GCIH
  - CompTia Security+, Network +, Project +

DISCUSSION

- What is an array?
- Creating, Adding to, and Indexing data in arrays
- Exporting and Importing data with arrays
- Processing data in an array to take an action

Examples will be discussed and demonstrated in PowerShell. Follow along if you like!

DISCLAIMER

- PowerShell scripts referenced in slides available on GitHub. Please do not use the scripts in production until you understand how they work in test environment.

WHAT IS AN ARRAY?

- A list or collection of objects or variables stored in memory
- No fixed length or size parameters
- Single item in an array often called “element”
- $array = @ ()
- Very powerful way to organize and process data sets

WHAT IS AN ARRAY?

CREATING AN ARRAY

```
PS > $StanleyCups = @(”Blackhawks”,6,”Captials”,1)
PS>  $StanleyCups
Blackhawks
6
Capitals
1
PS > $StanleyCups.Count
4 (elements)
PS>
```

WHAT IS AN ARRAY?

CREATING AN ARRAY

```
PS > $PresidentsTrophies = @(“Blackhawks”,1,”Captials”,2)
PS > $PresidentsTrophies
Blackhawks
2
Capitals
3
PS> $PresidentsTrophies.Count
4 (elements)
PS>
```

WHAT IS AN ARRAY?

ADDING TO AN ARRAY

Using the += operator, we can add or append data to an existing array.

Ability to add objects, variables, strings, or integers.

```
PS>$StanleyCups += (“Bruins”,6)
PS>$StanleyCups
Blackhawks
6
Capitals
1
Bruins
6
PS>
```

*For extra fun, use $Bruins=@(“Bruins”,3); $PresidentsTrophies += $Bruins

WHAT IS AN ARRAY?
INDEXING INTO ARRAYS

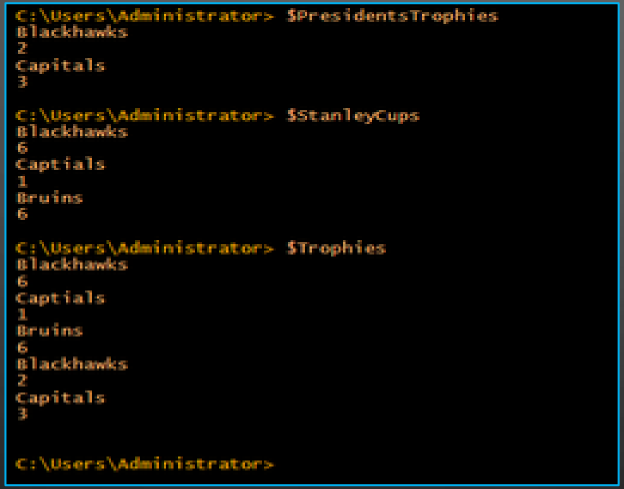
- Arrays are indexed using 0 based number scale
- Reference the first element in the array using [0], for the second element, [1]
- Or you can say, if you have 6 elements in the array, the first is [0] and the last is [5]

```
PS>$StanleyCups.Count
6
PS>$StanleyCups[0]
Blackhawks
PS>$StanleyCups[2]
Capitals
PS>
```

WHAT IS AN ARRAY?
INDEXING INTO ARRAYS CONTINUED

- Can you make an array of arrays? Yes we can!

```
PS> $Trophies=($StanleyCups, $PresidentsTrophies)
PS> $Trophies
```



```
C:\Users\Administrator> $PresidentsTrophies
Blackhawks
2
Capitals
3

C:\Users\Administrator> $StanleyCups
Blackhawks
6
Captials
1
Bruins
6

C:\Users\Administrator> $Trophies
Blackhawks
6
Captials
1
Bruins
6
Blackhawks
2
Capitals
3


C:\Users\Administrator>
```

@CRASH0VER1D3
HTTPS://GITHUB.COM/CRASH0VER1D3

EXPORTING AND IMPORTING DATA WITH ARRAYS

- Import-csv and Export-csv PowerShell cmdlets
- Store data for offline archive
- Create detailed reports
- Pass data as pipeline object with | operator
- HTML, JSON, CSV formats supported

EXPORTING AND IMPORTING DATA WITH ARRAYS EXPORT-CSV

```
PS> $Processes = Get-Process
```

The Get-Process cmdlet created an object with values, for each process

Storing into variable created a collection of these objects. Also known as array.

```
PS> $Processes.Count  (Results will vary, based on system)
PS> $Processes | export-csv .\Processes.csv

PS> $Processes = $null
```

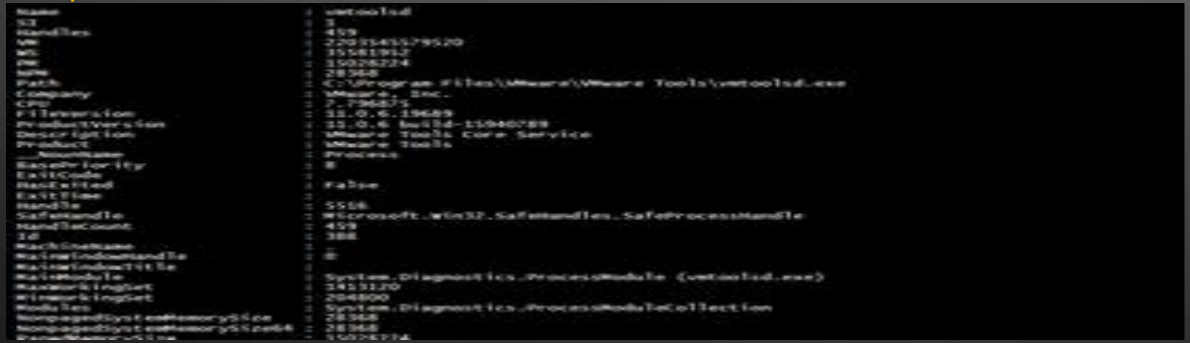
Cleared the variable contents from memory

EXPORTING AND IMPORTING DATA WITH ARRAYS IMPORT-CSV

```
PS> $Processes
```

All gone!

```
PS> $Processes = import-csv –path .\Processes.csv
PS>$Processes
```

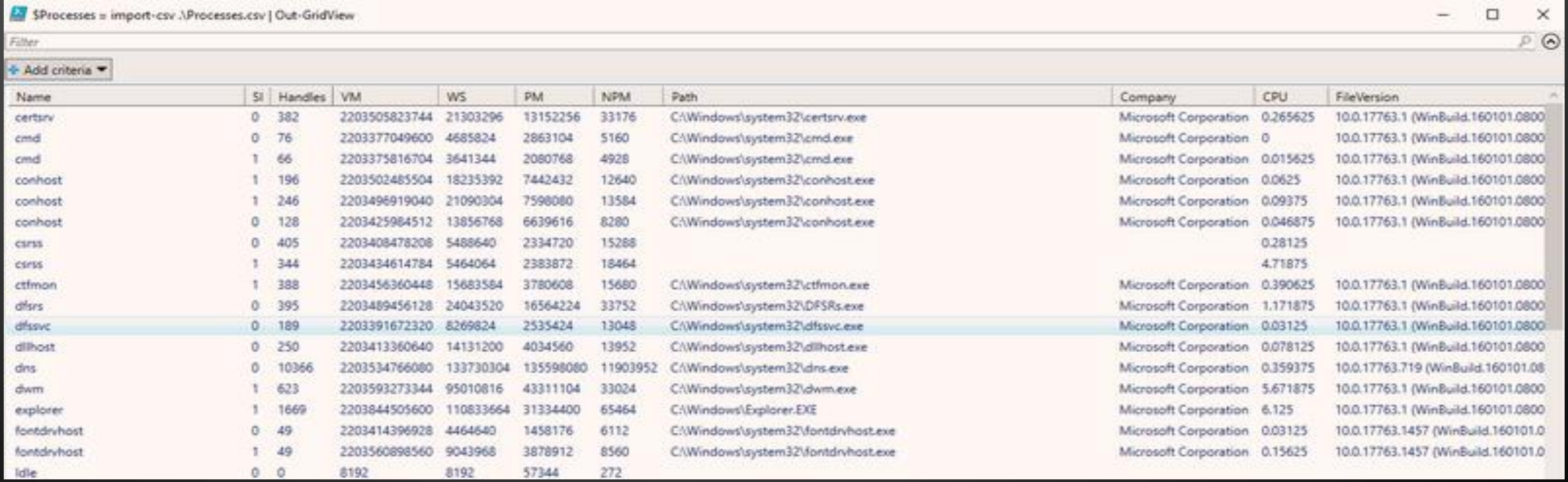


```
Name                       : vmtoolsd
SI                         : 1
Handles                    : 459
VM                         : 2203145579520
WS                         : 35581952
PM                         : 15028224
NPM                        : 28368
Path                       : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
Company                    : VMware, Inc.
CPU                        : 7.796875
FileVersion                : 11.0.6.19689
ProductVersion             : 11.0.6 build-15940789
Description                : VMware Tools Core Service
Product                    : VMware Tools
__NounName                 : Process
BasePriority               : 8
ExitCode                   :
HasExited                  : False
ExitTime                   :
Handle                     : 5516
SafeHandle                 : Microsoft.Win32.SafeHandles.SafeProcessHandle
HandleCount                : 459
Id                         : 388
MachineName                : .
MainWindowHandle           : 0
MainWindowTitle            :
MainModule                 : System.Diagnostics.ProcessModule (vmtoolsd.exe)
MaxWorkingSet              : 1413120
MinWorkingSet              : 204800
Modules                    : System.Diagnostics.ProcessModuleCollection
NonpagedSystemMemorySize   : 28368
NonpagedSystemMemorySize64 : 28368
PagedMemorySize            : 15028224
```

@CRASH0VER1D3
HTTPS://GITHUB.COM/CRASH0VER1D3

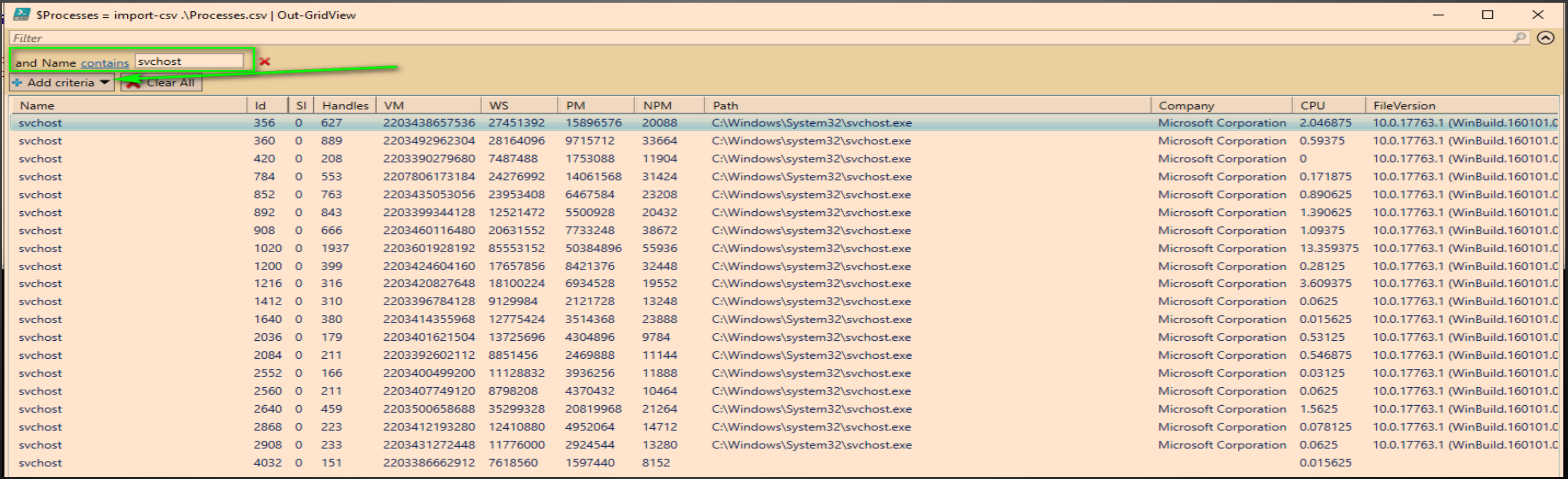
EXPORTING AND IMPORTING DATA WITH ARRAYS TIPS AND TRICKS

```
$Processes = import-csv –path .\Processes.csv | out-gridview
```



Name	SI	Handles	VM	WS	PM	NPM	Path	Company	CPU	FileVersion
certsrv	0	382	2203505823744	21303296	13152256	33176	C:\Windows\system32\certsrv.exe	Microsoft Corporation	0.265625	10.0.17763.1 (WinBuild.160101.0800
cmd	0	76	2203377049600	4685824	2863104	5160	C:\Windows\system32\cmd.exe	Microsoft Corporation	0	10.0.17763.1 (WinBuild.160101.0800
cmd	1	66	2203375816704	3641344	2080768	4928	C:\Windows\system32\cmd.exe	Microsoft Corporation	0.015625	10.0.17763.1 (WinBuild.160101.0800
conhost	1	196	2203502485504	18235392	7442432	12640	C:\Windows\system32\conhost.exe	Microsoft Corporation	0.0625	10.0.17763.1 (WinBuild.160101.0800
conhost	1	246	2203496919040	21090304	7598080	13584	C:\Windows\system32\conhost.exe	Microsoft Corporation	0.09375	10.0.17763.1 (WinBuild.160101.0800
conhost	0	128	2203425984512	13856768	6639616	8280	C:\Windows\system32\conhost.exe	Microsoft Corporation	0.046875	10.0.17763.1 (WinBuild.160101.0800
csrss	0	405	2203408478208	5488640	2334720	15288			0.28125	
csrss	1	344	2203434614784	5464064	2383872	18464			4.71875	
ctfmon	1	388	2203456360448	15683584	3780608	15680	C:\Windows\system32\ctfmon.exe	Microsoft Corporation	0.390625	10.0.17763.1 (WinBuild.160101.0800
dfsrs	0	395	2203489456128	24043520	16564224	33752	C:\Windows\system32\DFSRs.exe	Microsoft Corporation	1.171875	10.0.17763.1 (WinBuild.160101.0800
dfssvc	0	189	2203391672320	8269824	2535424	13048	C:\Windows\system32\dfssvc.exe	Microsoft Corporation	0.03125	10.0.17763.1 (WinBuild.160101.0800
dllhost	0	250	2203413360640	14131200	4034560	13952	C:\Windows\system32\dllhost.exe	Microsoft Corporation	0.078125	10.0.17763.1 (WinBuild.160101.0800
dns	0	10366	2203534766080	133730304	135598080	11903952	C:\Windows\system32\dns.exe	Microsoft Corporation	0.359375	10.0.17763.719 (WinBuild.160101.08
dwm	1	623	2203593273344	95010816	43311104	33024	C:\Windows\system32\dwm.exe	Microsoft Corporation	5.671875	10.0.17763.1 (WinBuild.160101.0800
explorer	1	1669	2203844505600	110833664	31334400	65464	C:\Windows\Explorer.EXE	Microsoft Corporation	6.125	10.0.17763.1 (WinBuild.160101.0800
fontdrvhost	0	49	2203414396928	4464640	1458176	6112	C:\Windows\system32\fontdrvhost.exe	Microsoft Corporation	0.03125	10.0.17763.1457 (WinBuild.160101.0
fontdrvhost	1	49	2203560898560	9043968	3878912	8560	C:\Windows\system32\fontdrvhost.exe	Microsoft Corporation	0.15625	10.0.17763.1457 (WinBuild.160101.0
Idle	0	0	8192	8192	57344	272				

EXPORTING AND IMPORTING DATA WITH ARRAYS TIPS AND TRICKS



$Processes = import-csv .\Processes.csv | Out-GridView

and Name contains svchost

Name	Id	SI	Handles	VM	WS	PM	NPM	Path	Company	CPU	FileVersion
svchost	356	0	627	2203438657536	27451392	15896576	20088	C:\Windows\System32\svchost.exe	Microsoft Corporation	2.046875	10.0.17763.1 (WinBuild.160101.0
svchost	360	0	889	2203492962304	28164096	9715712	33664	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.59375	10.0.17763.1 (WinBuild.160101.0
svchost	420	0	208	2203390279680	7487488	1753088	11904	C:\Windows\system32\svchost.exe	Microsoft Corporation	0	10.0.17763.1 (WinBuild.160101.0
svchost	784	0	553	2207806173184	24276992	14061568	31424	C:\Windows\System32\svchost.exe	Microsoft Corporation	0.171875	10.0.17763.1 (WinBuild.160101.0
svchost	852	0	763	2203435053056	23953408	6467584	23208	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.890625	10.0.17763.1 (WinBuild.160101.0
svchost	892	0	843	2203399344128	12521472	5500928	20432	C:\Windows\system32\svchost.exe	Microsoft Corporation	1.390625	10.0.17763.1 (WinBuild.160101.0
svchost	908	0	666	2203460116480	20631552	7733248	38672	C:\Windows\system32\svchost.exe	Microsoft Corporation	1.09375	10.0.17763.1 (WinBuild.160101.0
svchost	1020	0	1937	2203601928192	85553152	50384896	55936	C:\Windows\system32\svchost.exe	Microsoft Corporation	13.359375	10.0.17763.1 (WinBuild.160101.0
svchost	1200	0	399	2203424604160	17657856	8421376	32448	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.28125	10.0.17763.1 (WinBuild.160101.0
svchost	1216	0	316	2203420827648	18100224	6934528	19552	C:\Windows\system32\svchost.exe	Microsoft Corporation	3.609375	10.0.17763.1 (WinBuild.160101.0
svchost	1412	0	310	2203396784128	9129984	2121728	13248	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.0625	10.0.17763.1 (WinBuild.160101.0
svchost	1640	0	380	2203414355968	12775424	3514368	23888	C:\Windows\System32\svchost.exe	Microsoft Corporation	0.015625	10.0.17763.1 (WinBuild.160101.0
svchost	2036	0	179	2203401621504	13725696	4304896	9784	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.53125	10.0.17763.1 (WinBuild.160101.0
svchost	2084	0	211	2203392602112	8851456	2469888	11144	C:\Windows\System32\svchost.exe	Microsoft Corporation	0.546875	10.0.17763.1 (WinBuild.160101.0
svchost	2552	0	166	2203400499200	11128832	3936256	11888	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.03125	10.0.17763.1 (WinBuild.160101.0
svchost	2560	0	211	2203407749120	8798208	4370432	10464	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.0625	10.0.17763.1 (WinBuild.160101.0
svchost	2640	0	459	2203500658688	35299328	20819968	21264	C:\Windows\System32\svchost.exe	Microsoft Corporation	1.5625	10.0.17763.1 (WinBuild.160101.0
svchost	2868	0	223	2203412193280	12410880	4952064	14712	C:\Windows\system32\svchost.exe	Microsoft Corporation	0.078125	10.0.17763.1 (WinBuild.160101.0
svchost	2908	0	233	2203431272448	11776000	2924544	13280	C:\Windows\System32\svchost.exe	Microsoft Corporation	0.0625	10.0.17763.1 (WinBuild.160101.0
svchost	4032	0	151	2203386662912	7618560	1597440	8152			0.015625	

@CRASH0VER1D3
HTTPS://GITHUB.COM/CRASH0VER1D3

PROCESSING DATA IN AN ARRAY TO TAKE AN ACTION SOME USE CASES

- Use comparison operators to find properties that meet your criteria
  -eq –ne –gt –lt –like –nlike –match

Take action based on criteria match
-Add object to another report (filtering)

-Delete a process

-Disable a user account

-Create log entry

PROCESSING DATA IN AN ARRAY TO TAKE AN ACTION

Let’s create a new process to use in our next example. Do this as Admin

```
PS>wmic process call create cmd
Executing (Win32_Process)->Create()
Method execution successful.
```

If you want to turn it up a notch, run the command several times

NOTE:If you are using ISE, you will see an error as well, NativeCommandError

PROCESSING DATA IN AN ARRAY TO TAKE AN ACTION

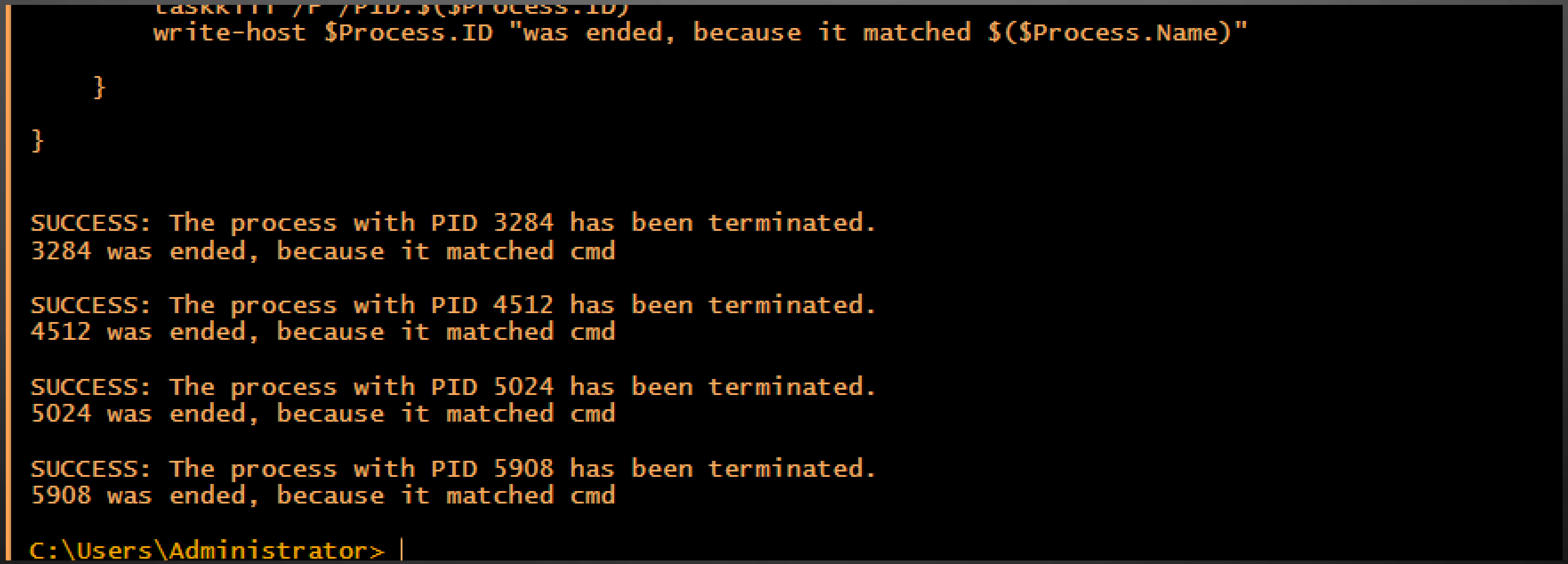
```
$Processes = import-csv –path .\Processes.csv

Foreach ($Process in $Processes)
{
        write-host
        write-host $Process.Name
        write-host $Process.Path
        write-host $Process.Id
}
```

PROCESSING DATA IN AN ARRAY TO TAKE AN ACTION

```
Foreach ($Process in $Processes)
{
        if ($Process.Name –like “cmd”)
        {
                write-host
                taskkill /F /PID:$($Process.ID)
                write-host $Process.ID “was ended, because it matched $($Process.Name)”
        }
}
```

CONGRATULATIONS, YOU JUST AUTOMATED AN ACTION USING POWERSHELL AND ARRAYS!



```
        taskkill /F /PID:$($Process.ID)
        write-host $Process.ID "was ended, because it matched $($Process.Name)"

    }

}


SUCCESS: The process with PID 3284 has been terminated.
3284 was ended, because it matched cmd

SUCCESS: The process with PID 4512 has been terminated.
4512 was ended, because it matched cmd

SUCCESS: The process with PID 5024 has been terminated.
5024 was ended, because it matched cmd

SUCCESS: The process with PID 5908 has been terminated.
5908 was ended, because it matched cmd

C:\Users\Administrator> |
```

@CRASHOVER1D3
HTTPS://GITHUB.COM/CRASHOVER1D3

CLOSING THOUGHTS

- Learning how to manipulate arrays can be a gamechanger
- Increases accuracy
- Reduces overall effort to accomplish tasks at scale
- Automation enables us generate repeatable results
- Sky is the limit
- Everyone deserves arrays!

@CRASH0VER1D3
HTTPS://GITHUB.COM/CRASH0VER1D3