

Christmas Cheer Laser, part 7

Answer to the Previous Question

- 8) What is the next riddle? Note the part of this riddle, “then you /shall/see.”

~~Get-Process -username~~

```
PS /home/elf> Get-Process -Username
Get-Process : A parameter cannot be found that matches parameter name 'Username'.
At line:1 char:13
+ Get-Process -Username
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Get-Process], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.GetProcessCommand
```

```
PS /home/elf> Get-Process | Get-Member
```

Name	MemberType	Definition
Handles	AliasProperty	Handles = Handlecount
Name	AliasProperty	Name = ProcessName
NPM	AliasProperty	NPM = NonpagedSystemMemorySize64
PM	AliasProperty	PM = PagedMemorySize64

Hmm, Username is not valid. Time for the search engine. <https://thinkpowershell.com/get-process-name-and-owner-user-name/> tells us to use -IncludeUserName.

Get-Process -IncludeUserName

```
PS /home/elf> Get-Process -IncludeUserName
```

WS (M)	CPU(s)	Id	UserName	ProcessName
28.96	0.91	6	root	CheerLaserServi
115.74	2.56	31	elf	elf
3.62	0.03	1	root	init
0.71	0.00	23	bushy	sleep
0.71	0.00	26	alabaster	sleep
0.72	0.00	27	minty	sleep
0.72	0.00	29	holly	sleep
3.49	0.00	30	root	su

```
PS /home/elf>
```

We just need to kill the processes in order, bushy, alabaster, minty, and holly. It turns out you don't even have to write a script, doing it by hand works.

```

PS /home/elf> Get-Process -IncludeUserName

    WS (M)    CPU(s)    Id  UserName    ProcessName
    -----
    28.96      0.91      6   root        CheerLaserServi
    115.74     2.56     31   elf         elf
    3.62       0.03      1   root        init
    0.71       0.00     23   bushy       sleep
    0.71       0.00     26   alabaster   sleep
    0.72       0.00     27   minty       sleep
    0.72       0.00     29   holly       sleep
    3.49       0.00     30   root        su

PS /home/elf> Stop-Process 23
PS /home/elf> Stop-Process 26
PS /home/elf> Stop-Process 27
PS /home/elf> Stop-Process 29
PS /home/elf> Get-Process -IncludeUserName

    WS (M)    CPU(s)    Id  UserName    ProcessName
    -----
    27.33      1.09      6   root        CheerLaserServi
    114.79     2.77     31   elf         elf
    3.62       0.03      1   root        init
    3.49       0.00     30   root        su

PS /home/elf>

```

The hint, “then you /shall/see.” was telling us to get the content of /shall/see.

```

PS /> dir /shall/see

Directory: /shall

Mode                LastWriteTime         Length Name
----                -
--r--              1/13/20   9:59 PM         149 see

PS /> Get-Content /shall/see
Get the .xml children of /etc - an event log to be found. Group all .Id's and the last thing will be
in the Properties of the lonely unique event Id.

PS />

```

Wow, another riddle. Does this ever stop?

The .xml file you will find is very long, as each event has about 200 lines and there are 1200 events. You may use XML commands, write a script or just take a shot at searching for something you know should be in the file.

Note: It looks strange, but if you are searching for text files, `dir /folder/*.txt` works well.

Question

- 9) What laser parameters do you recover from the XML document?