

## Christmas Cheer Laser, part 2

### PowerShell Aliases

PowerShell cmdlets are in the form, Verb-Noun. For example, the command to read the contents of a file is `Get-Content`. To those used to using `cat` in Linux or `type` in Windows, that seems like a lot of typing. PowerShell gives us aliases to reduce typing. Often, the equivalent commands in Linux or Windows are available as aliases. To see the aliases for a command, use

`Get-Alias -Definition {cmdlet}`

For example, this shows the aliases for `Get-Content`.

```
PS /home/elf> Get-Alias -Definition Get-Content

CommandType      Name                                Version      Source
-----
Alias             gc -> Get-Content
Alias             type -> Get-Content

PS /home/elf>
```

In PowerShell v. 5 on Windows, `cat` is also an alias for `Get-Content`. It could be that Linux aliases have been removed from this terminal to force players to use Windows commands.

### Answers to Previous Questions

- 1) Read the attacker's taunting note. What command would access the data he suggests we look at?

```
PS /home/elf> gc /home/callingcard.txt
What's become of your dear laser?
Fa la la la la, la la la la
Seems you can't now seem to raise her!
Fa la la la la, la la la la
Could commands hold riddles in hist'ry?
Fa la la la la, la la la la
Nay! You'll ever suffer myst'ry!
Fa la la la la, la la la la
PS /home/elf>
```

The attacker says that commands hold riddles in hist'ry. They are referring to the command history. A quick query to your favorite search engine will tell you the cmdlet you need is `Get-History`.

- 2) Use the PowerShell command for getting a web page, `Invoke-WebRequest`, to see the status of the laser (the command is in red in the laser terminal.) What parameters will we have to find to correctly calibrate the laser? Hint: one of them is lens refraction, or refraction.

You can copy and paste the command you need from the terminal.

```
(Invoke-WebRequest -Uri http://localhost:1225/).RawContent
```

```

PS /home/elf> (Invoke-WebRequest -Uri http://localhost:1225/).RawContent
HTTP/1.0 200 OK
Server: Werkzeug/0.16.0
Server: Python/3.6.9
Date: Mon, 13 Jan 2020 14:43:31 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 860

<html>
<body>
<pre>
-----
Christmas Cheer Laser Project Web API
-----

Turn the laser on/off:
GET http://localhost:1225/api/on
GET http://localhost:1225/api/off

Check the current Mega-Jollies of laser output
GET http://localhost:1225/api/output

Change the lense refraction value (1.0 - 2.0):
GET http://localhost:1225/api/refraction?val=1.0

Change laser temperature in degrees Celsius:
GET http://localhost:1225/api/temperature?val=-10

Change the mirror angle value (0 - 359):
GET http://localhost:1225/api/angle?val=45.1

Change gaseous elements mixture:
POST http://localhost:1225/api/gas
POST BODY EXAMPLE (gas mixture percentages):
O=5&H=5&He=5&N=5&Ne=20&Ar=10&Xe=10&F=20&Kr=10&Rn=10
-----
</pre>
</body>
</html>
PS /home/elf>

```

The values we will need to recalibrate the laser are refraction, temperature, angle, and gas.

### Format-List

If you don't give it instructions, PowerShell will choose its own formatting for the output it displays. If it determines that there is not enough room to fit output on a line it will truncate the output and signify that by ending the data with an ellipsis (...). PowerShell has several cmdlets to help with formatting output, but two of them are `Format-List` and `Format-Table`. `Format-List` is especially handy for getting rid of ellipses; just pipe the output into `Format-List` (alias `fl`). For example, `Get-History | Format-List` or `Get-History | fl`

### Questions

- 3) Find the message (and a parameter, too) in the command History
  
- 4) The answer to the previous question includes, "name=value variables that I share to applications system wide." That's a strong hint to tell you where to look next. The terms "variables", "share to applications system wide", and "name=value" are all useful hints.