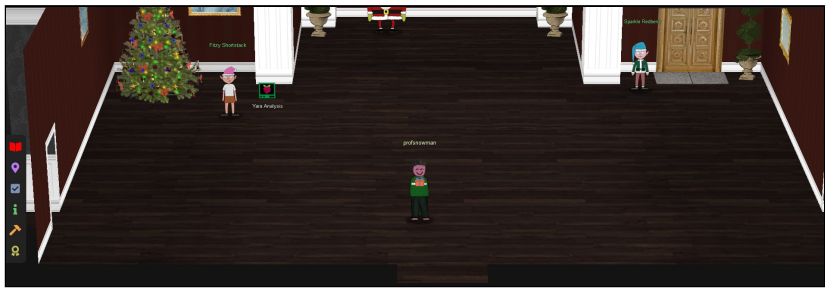
# KringleCon 4: Calling Birds!

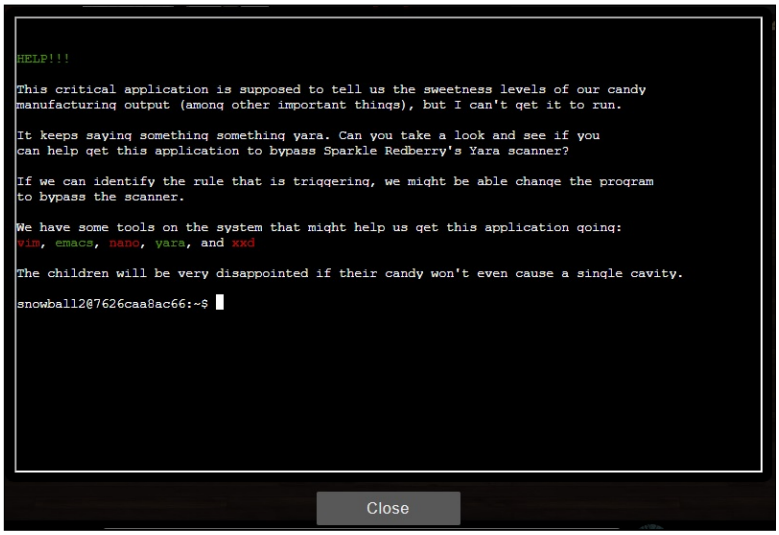
## Entry



1. Click to talk to `Fity Shortstack`

```
Hiya, I'm Fitzy Shortstack!

I was just trying to learn a bit more about YARA with this here Cranberry Pi terminal.

I mean, I'm not saying I'm worried about attack threats from that other con next door, but...

OK. I AM worried. I've been thinking a bit about how malware might bypass YARA rules.

If you can help me solve the issue in this terminal, I'll understand YARA so much better! Would
you please check it out so I can learn?

And, I'll tell you what - if you help me with YARA, I'll give you some tips for Splunk!

I think if you make small, innocuous changes to the executable, you can get it to run in spite of
the YARA rules.
```

2. Click `Yara Analysis` Cranberry Pi terminal



3. Type `ls`

```
the_critical_elf_app  yara_rules
```

4. Type `./the_critical_elf_app`

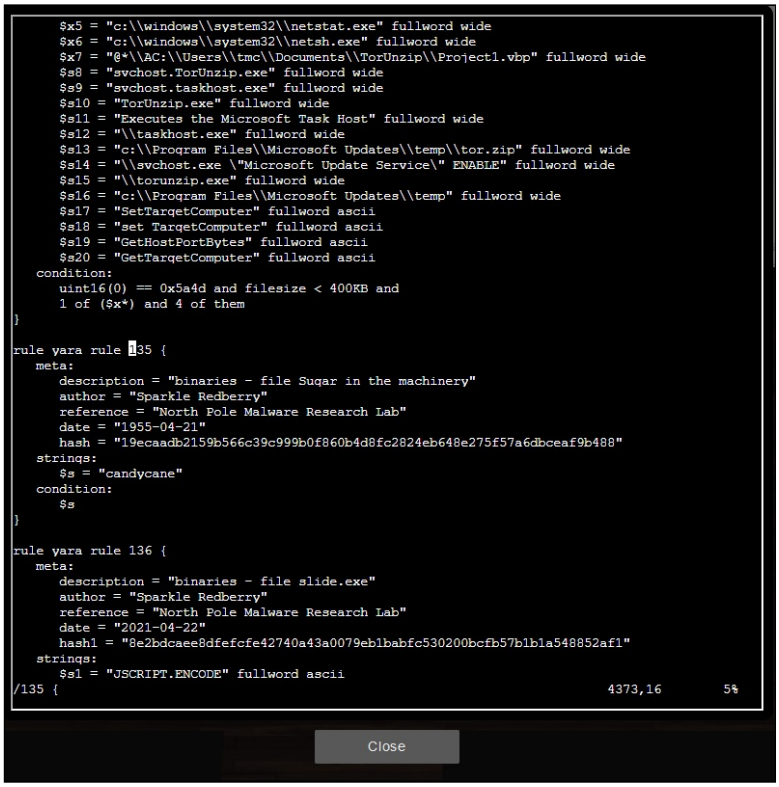
```
yara_rule_135 ./the_critical_elf_app
```

5. Type `ls yara_rules/`

```
rules.yar
```

6. Type `vi yara_rules/rules.yar`

7. Type `/135 {`




8. Close `vi`

9. Type `vi the_critical_elf_app`

10. Type `/candy`

11. Change candycane to `Candycane`

12. Save the modified file and close `vi`

13. Type `./the_critical_elf_app`

```
yara_rule_1056 ./the_critical_elf_app
```

14. Type `vi yara_rules/rules.yar`

15. Type `/1056 {`


| $s1 | ASCII |
|---|---|
| 6c 6962 632e 736f 2e36 | libc.so.6 |

| $hs2 | ASCII |
|---|---|
| 726f 6772 616d 2121 | rogram!! |

16. Close `vi`

17. Type `vi the_critical_elf_app`

18. Type `/rogram!!`

19. Change rogram!! to `orgram!!`

20. Save the modified file and close `vi`

21. Type `./the_critical_elf_app`

```
yara_rule_1732 ./the_critical_elf_app
```

22. Type `vi yara_rules/rules.yar`

23. Type `/1732 {`


24. Type `vi the_critical_elf_app`

25. Type `__frame`

26. Change the following

| String | Modified String |
|---|---|
| __frame_dummy_init_array_entry | `__frame_dummy_init_Array_entry` |
| .note.gnu.property | `.note.gnu.Property` |
| .eh_frame_hdr | `.eh_frame_Hdr` |
| *__FRAME_END__* | `__FRAME_eND__` |
| __GNU_EH_FRAME_HDR | `__GNU_EH_FRAME_hDR` |
| frame_dummy | `frame_Dummy` |
| .note.gnu.build-id | `.note.gnu.build-Id` |
| .note.ABI-tag | `.note.ABI-Tag` |
| naughty string | `naughty String` |
| dastardly string | `dastardly String` |
| __do_global_dtors_aux_fini_array_entry | `__do_global_dtors_aux_fini_array_Entry` |
| its_a_holly_jolly_variable | `its_a_Holly_jolly_variable` |

| String | Modified String |
| --- | --- |
| HolidayHackChallenge{NotReallyAFlag} | `HolidayHackChallenge{NotReallyaFlag}` |

27. Save the modified file and close `vi`
28. Type `./the_critical_elf_app`

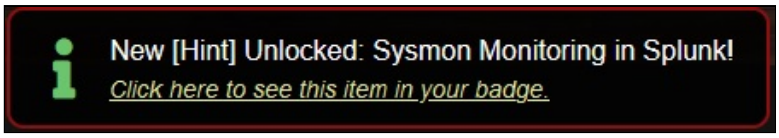
```
Machine Running..
Toy Levels: Very Merry, Terry
Naughty/Nice Blockchain Assessment: Untampered
Candy Sweetness Gauge: Exceedingly Sugarlicious
Elf Jolliness Quotient: 4a6f6c6c7920456e6f7567682c204f76657274696d6520417070726f766564
```


29. Click the `Close` button
30. Click to talk to `Fity Shortstack`

```
Thanks - you figured it out!

Let me tell you what I know about Splunk.

Did you know Splunk recently added support for new data sources including Sysmon for Linux and
GitHub Audit Log data?

Between GitHub audit log and webhook event recording, you can monitor all activity in a
repository, including common git commands such as git add, git status, and git commit.
```

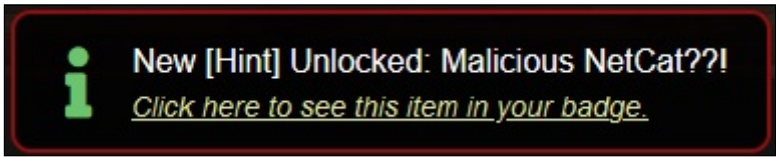

31. Click to talk to `Fity Shortstack`

```
You can also see cloned GitHub projects. There's a lot of interesting stuff out there. Did you
know there are repositories of code that are Darn Vulnerable?

Sysmon provides a lot of valuable data, but sometimes correlation across data types is still
necessary.

Sysmon network events don't reveal the process parent ID for example. Fortunately, we can pivot
with a query to investigate process creation events once you get a process ID.
```



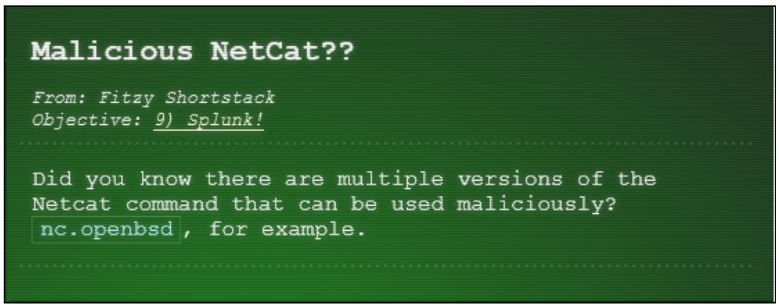

32. Click to talk to `Fity Shortstack`

> Sometimes Sysmon data collection is awkward. Pipelining multiple commands generates multiple Sysmon events, for example.
>
> Did you know there are multiple versions of the Netcat command that can be used maliciously? nc.openbsd, for example.

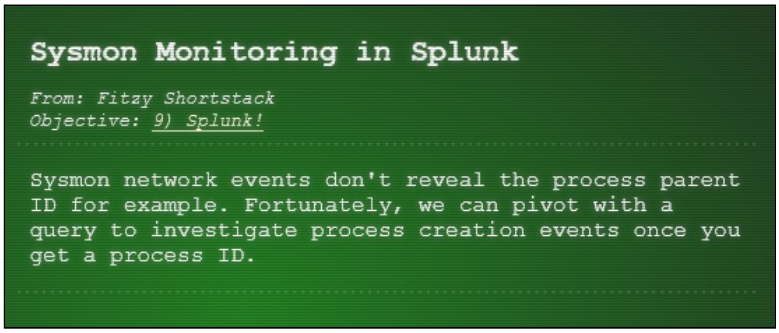



33. Click the `i` (Hints) icon

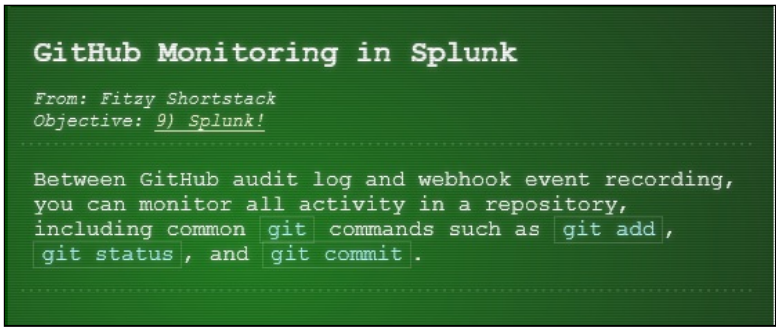
34. Click `Malicious NetCat??`




35. Click `Sysmon Monitoring in Splunk`




36. Click `GitHub Monitoring in Splunk`



37. Click `[Exit]`

38. Click to talk to `Sparkle Redberry`

```
Hey there! I’m Sparkle Redberry.

This year, the Santavator is in top working shape! We ironed out all of the issues from last year with it.

As for that tower next door, I hear they have an elevator of some sort too.

I just don't know if it would take me anywhere I'd really want to go.
```

39. Click the `Santavator`


41. Click `2` to move to the Talks Lobby

42. Click the `Santavator`

43. Click `3` to move to Santa's Office

44. Click the `Santavator`

45. Click `R` to move to NetWars

46. Click the `Santavator`

47. Click `*1` to move to the Lobby

48. Move `Left` and enter the `Dining Room`