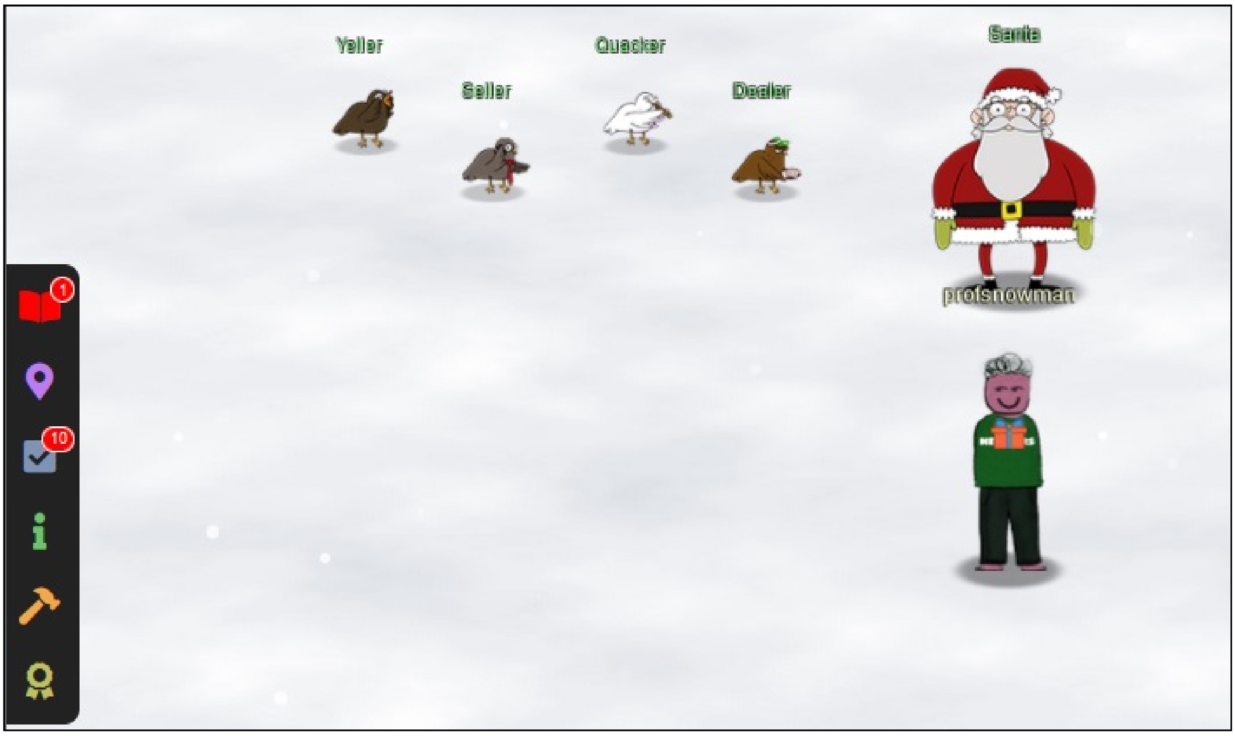
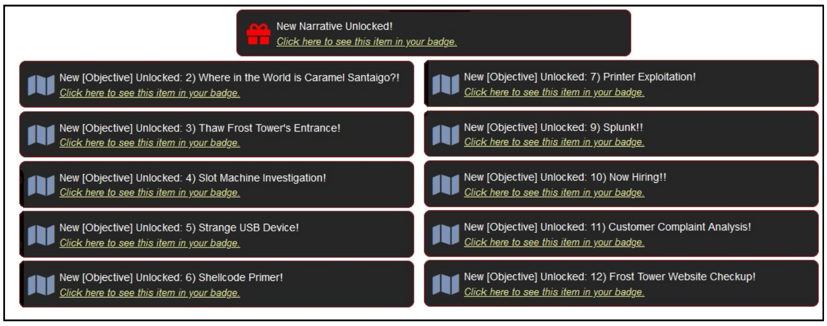
KringleCon 4: Calling Birds!

The North Pole





New Narrative Unlocked!
Click here to see this item in your badge.

New [Objective] Unlocked: 2) Where in the World is Caramel Santaigo?!
Click here to see this item in your badge.

New [Objective] Unlocked: 3) Thaw Frost Tower's Entrance!
Click here to see this item in your badge.

New [Objective] Unlocked: 4) Slot Machine Investigation!
Click here to see this item in your badge.

New [Objective] Unlocked: 5) Strange USB Device!
Click here to see this item in your badge.

New [Objective] Unlocked: 6) Shellcode Primer!
Click here to see this item in your badge.

New [Objective] Unlocked: 7) Printer Exploitation!
Click here to see this item in your badge.

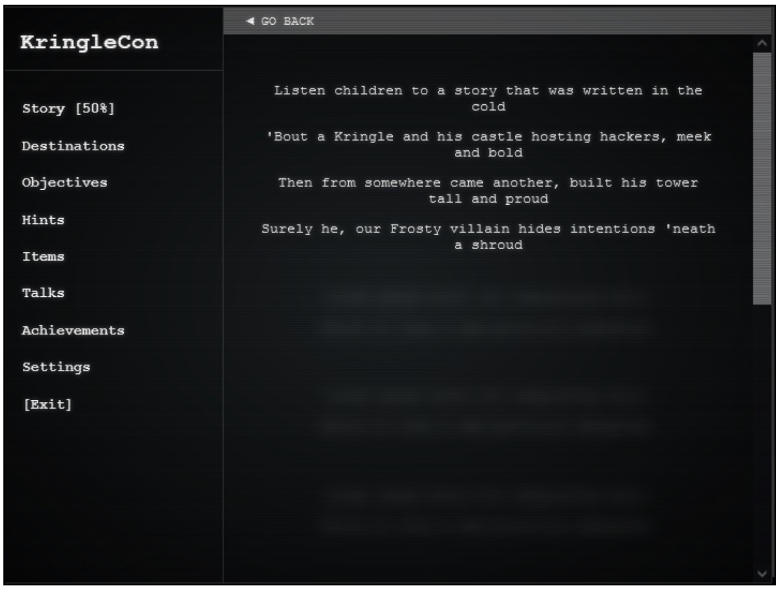
New [Objective] Unlocked: 9) Splunk!!
Click here to see this item in your badge.

New [Objective] Unlocked: 10) Now Hiring!!
Click here to see this item in your badge.

New [Objective] Unlocked: 11) Customer Complaint Analysis!
Click here to see this item in your badge.

New [Objective] Unlocked: 12) Frost Tower Website Checkup!
Click here to see this item in your badge.

1. Click the Book (Story) icon



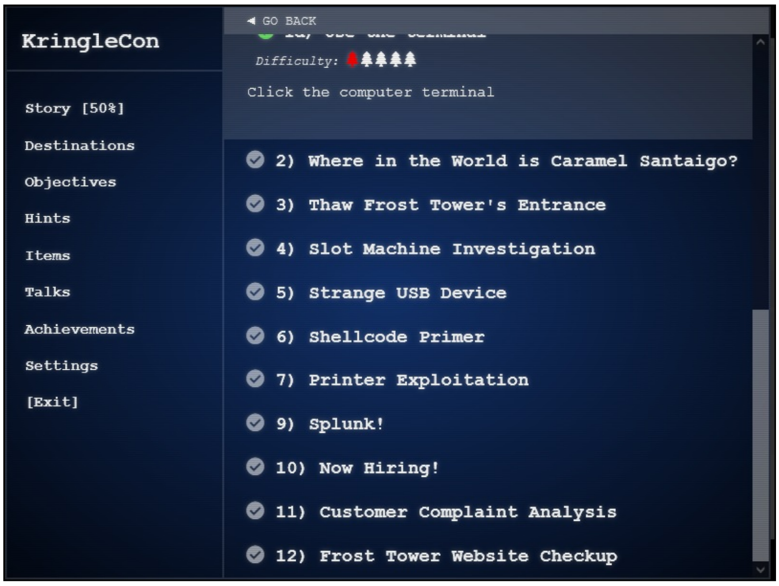
Listen children to a story that was written in the cold

'Bout a Kringle and his castle hosting hackers, meek and bold

Then from somewhere came another, built his tower tall and proud

Surely he, our Frosty villain hides intentions 'neath a shroud

2. Click `Objectives` and then scroll `Down`



Difficulty:

Click the computer terminal

2) Where in the World is Caramel Santaigo?

3) Thaw Frost Tower's Entrance

4) Slot Machine Investigation

5) Strange USB Device

6) Shellcode Primer

7) Printer Exploitation

9) Splunk!

10) Now Hiring!

11) Customer Complaint Analysis

12) Frost Tower Website Checkup

3. Click `[Exit]`

4. Click to talk to `Santa`

```
Ho ho ho! I'm Santa Claus!

Welcome to the North Pole and KringleCon IV: Calling Birds!

I’d like to introduce you to the four birds here, each of whom is calling.

We're so glad to have you here to celebrate the holidays - and practice some important skills.

What's that? You've heard of another conference up at the North Pole?

Well, I'm afraid you'll have to ask Jack Frost about that.

To be honest, I'm not quite sure what his intentions are, but I am keeping an eye out...

Anyway, enjoy your time with the SANS Holiday Hack Challenge and KringleCon!
```

5. Click to talk to `Dealer`

```
Ante up!
```

6. Click to talk to `Quacker`

```
QUACK!
```

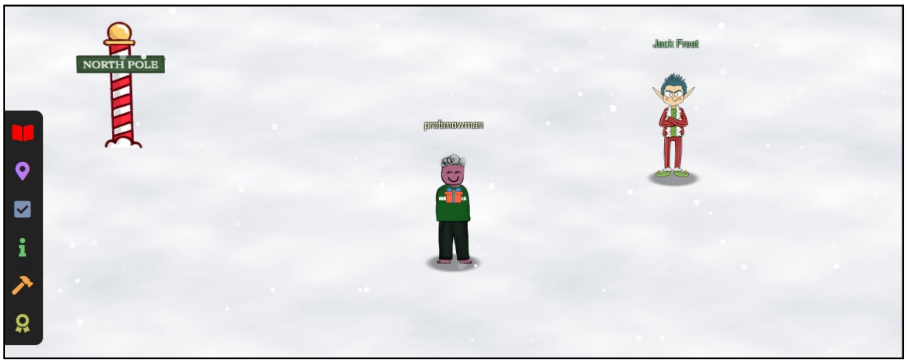
7. Click to talk to `Seller`

```
Your car's warranty is about to expire!
```

8. Click to talk to `Yeller`

```
HEEEEEEY YOU!!!
```

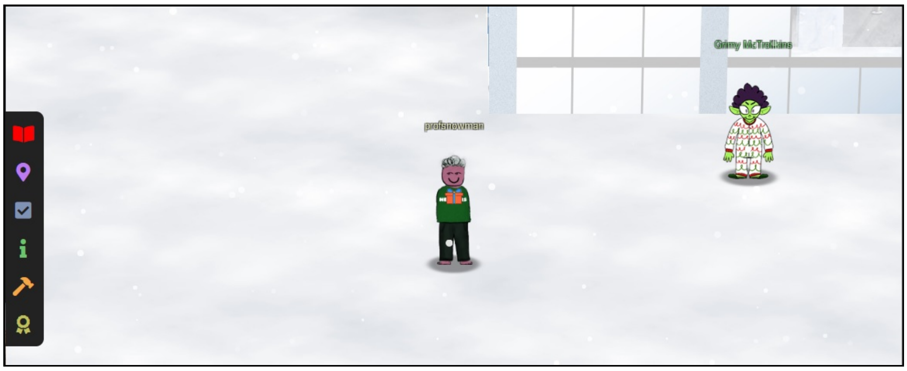
9. Move `Right`



10. Click to talk to `Jack Frost`

```
Welcome to the North Pole - the Frostiest Place on Earth™!

Last year, Santa somehow foiled my plot.

So this year, I've decided to beat Santa at his own game – I’m gonna take over the Holiday Season
from the old man and dominate it myself.

I've built Frost Tower, the epicenter of Frostiness at the North Pole. Believe me, it's the
BIGGEST North Pole tower the world has EVER seen! So much better than that lame castle next door.

And, quite frankly, our FrostFest conference is going to be the GREATEST con in the history of
cons.

As for FrostFest, we honor all badges for entry, including those from the lame conference next
door.

Oh, and make sure you visit the gift shop and buy some SWAG on your way out.

Everybody says it's the best SWAG you'll ever find! People love our swag!
```

11. Move Up

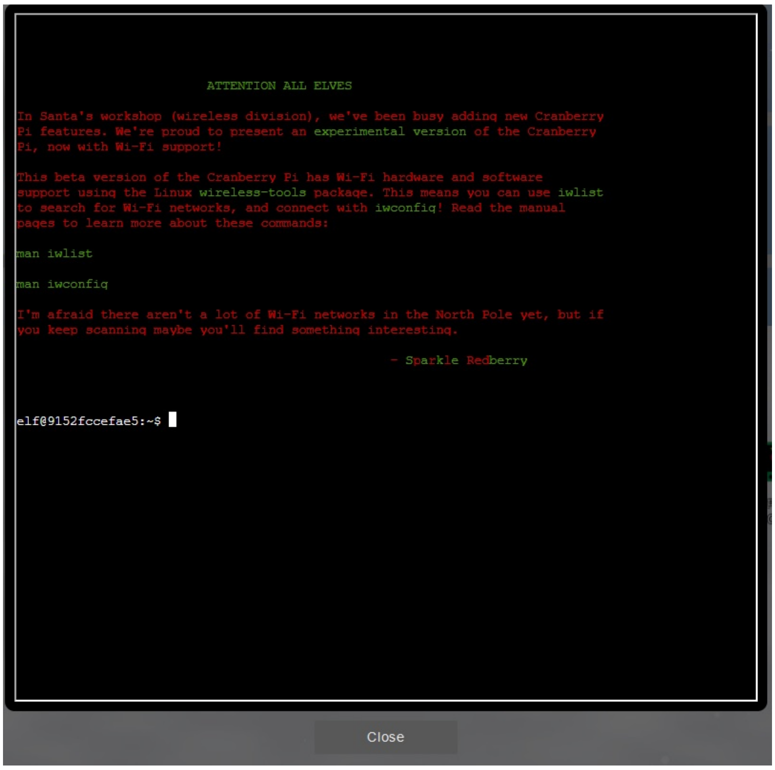


12. Click to talk to `Grimy McTrollkins`

```
Yo, I'm Grimy McTrollkins.

I'm a troll and I work for the big guy over there: Jack Frost.

I’d rather not be bothered talking with you, but I’m kind of in a bind and need your help.

Jack Frost is so obsessed with icy cold that he accidentally froze shut the door to Frost Tower!

I wonder if you can help me get back in.

I think we can melt the door open if we can just get access to the thermostat inside the
building.

That thermostat uses Wi-Fi. And I’ll bet you picked up a Wi-Fi adapter for your badge when you
got to the North Pole.

Click on your badge and go to the Items tab. There, you should see your Wi-Fi Dongle and a button
to “Open Wi-Fi CLI.” That’ll give you command-line interface access to your badge’s wireless
capabilities.
```

13. Click `Hammer` (Items) icon

14. Click `Open WiFi CLI`



```
                          ATTENTION ALL ELVES

In Santa's workshop (wireless division), we've been busy adding new Cranberry
Pi features. We're proud to present an experimental version of the Cranberry
Pi, now with Wi-Fi support!

This beta version of the Cranberry Pi has Wi-Fi hardware and software
support using the Linux wireless-tools package. This means you can use iwlist
to search for Wi-Fi networks, and connect with iwconfig! Read the manual
pages to learn more about these commands:

man iwlist

man iwconfig

I'm afraid there aren't a lot of Wi-Fi networks in the North Pole yet, but if
you keep scanning maybe you'll find something interesting.

                                                     - Sparkle Redberry



elf@9152fccefae5:~$
```

15. Type `iwlist wlan0 scanning`

16. Type `iwconfig wlan0 essid "FROST-Nidus-Setup"`

17. Type `curl http://nidus-setup:8080/`

18. Type `curl http://nidus-setup:8080/apidoc`

19. Type `curl -XPOST -H 'Content-Type: application/json' \`

20. Type `--data-binary '{"temperature": 1}' \`

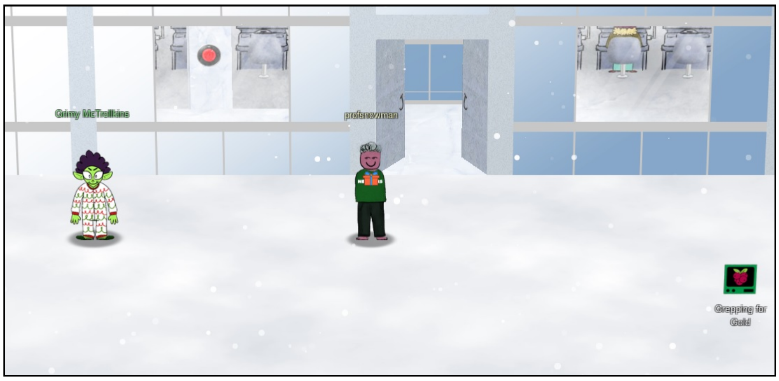
21. Type `http://nidus-setup:8080/api/coolercurl`

```
{
  "temperature": 0.27,
  "humidity": 32.15,
  "wind": 3.28,
  "windchill": -0.33,
  "WARNING": "ICE MELT DETECTED!"
}
```

New [Achievement] Unlocked: Thaw Frost Tower's Entrance!

Click here to see this item in your badge.

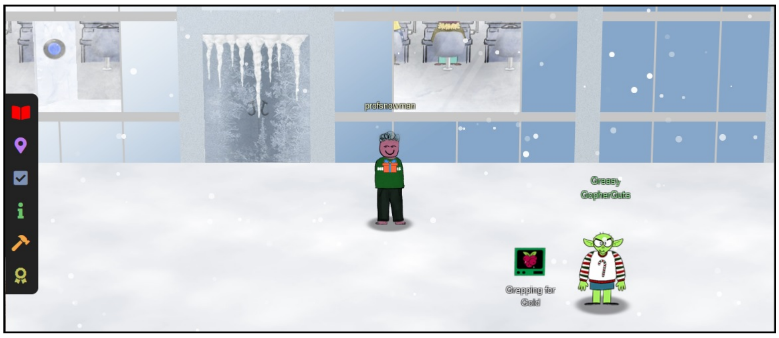
22. Click the `Close` button



23. Click to talk to `Grimy McTrollkins`

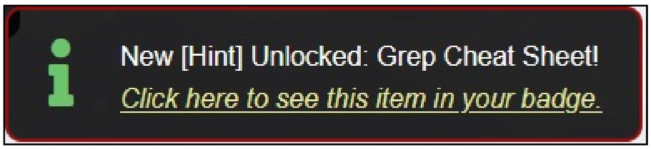
```
Great - now I can get back in!
```

24. Move `Right`



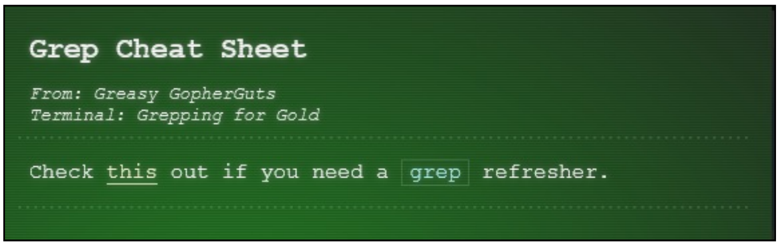
25. Click to talk to `Greasy GopherGuts`

```
Grnph. Blach! Phlegm.

I'm Greasy Gopherguts. I need help with parsing some Nmap output.
```



New [Hint] Unlocked: Grep Cheat Sheet!
Click here to see this item in your badge.

26. Click the `i` (Hints) icon



Grep Cheat Sheet

From: Greasy GopherGuts
Terminal: Grepping for Gold

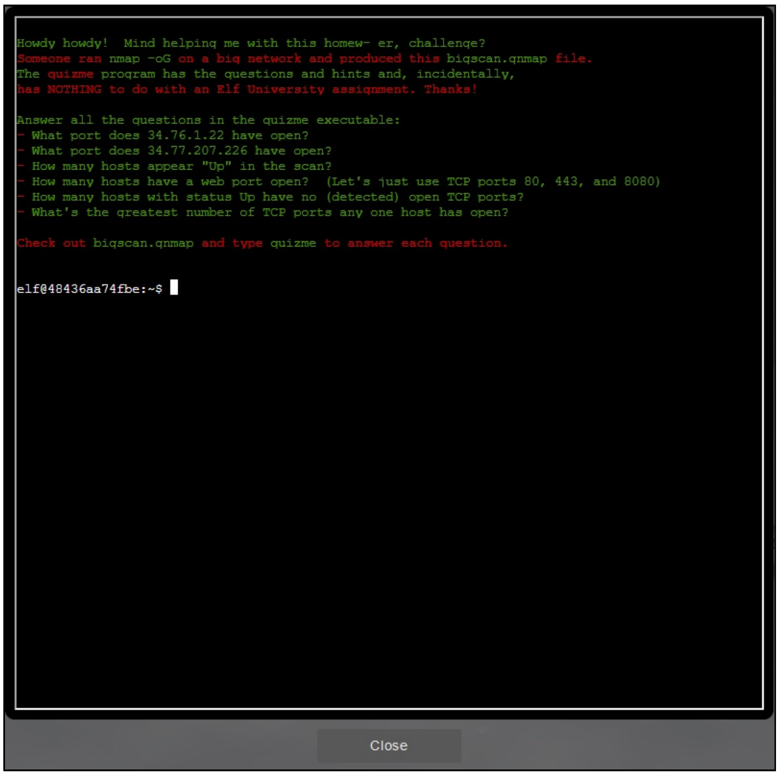
Check this out if you need a `grep` refresher.

27. Click `[Exit]`

28. Click to talk to `Greasy GopherGuts`

```
If you help me find some results, I'll give you some hints about Wi-Fi.

Click on the terminal next to me and read the instructions.

Maybe search for a cheat sheet if the hints in the terminal don't do it for ya'.

You’ll type quizme in the terminal and grep through the Nmap bigscan.gnmap file to find answers.
```

29. Click `Grepping for Gold` Cranberry Pi terminal



```
Howdy howdy!  Mind helping me with this homew- er, challenge?
Someone ran nmap -oG on a big network and produced this bigscan.gnmap file.
The quizme program has the questions and hints and, incidentally,
has NOTHING to do with an Elf University assignment. Thanks!

Answer all the questions in the quizme executable:
- What port does 34.76.1.22 have open?
- What port does 34.77.207.226 have open?
- How many hosts appear "Up" in the scan?
- How many hosts have a web port open?  (Let's just use TCP ports 80, 443, and 8080)
- How many hosts with status Up have no (detected) open TCP ports?
- What's the greatest number of TCP ports any one host has open?

Check out bigscan.gnmap and type quizme to answer each question.


elf@48436aa74fbe:~$
```

30. Type `grep 34.76.1.22 bigscan.gnmap`

```
Host: 34.76.1.22 ()	Status: Up
Host: 34.76.1.22 ()	Ports: 62078/open/tcp//iphone-sync///	Ignored State: closed (999)
```

31. Type `quizme`

```
What port does 34.76.1.22 have open?
Please enter your answer or press h for a hint:
```

32. Type `62078`

```
That's correct!
We used this as a solution:
grep 34.76.1.22 bigscan.gnmap
This looks for "34.76.1.22" in the bigscan.gnmap file and shows us every place where it shows up.
In the results, we see:
   62078/open/tcp//iphone-sync///
This tells us port TCP 62078 was found open by nmap.
You have 5 challenges left.
```

33. Type `grep 34.77.207.226 bigscan.gnmap`

```
Host: 34.77.207.226 ()     Status: Up
Host: 34.77.207.226 ()     Ports: 8080/open/tcp//http-proxy///      Ignored State: filtered (999)
```

34. Type `quizme`

```
What port does 34.77.207.226 have open?
Please enter your answer or press h for a hint:
```

35. Type `8080`

```
That's correct!
We used this as a solution:
grep 34.77.207.226 bigscan.gnmap
Like the previous challenge, this searches the nmap output file for a specific IP address.  In
the output, we see TCP port 8080 is open:
  8080/open/tcp//http-proxy///
You have 4 challenges left.
```

36. type `grep Up bigscan.gnmap | wc -l`

```
26054
```

37. Type `quizme`

```
How many hosts appear "Up" in the scan?
Please enter your answer or press h for a hint:
```

38. Type `26054`

```
That's correct!
We used this as a solution:
grep Up bigscan.gnmap | wc -l
Running the grep part of the command returns every line with "Up" in it, and wc counts the bytes,
characters, words, and lines that come out of grep. Using "-l" only shows lines.
You have 3 challenges left.
```

39. Type `grep -E "(80/open|443/open|8080/open)" bigscan.gnmap | wc -l`

```
14372
```

40. Type `quizme`

```
How many hosts have a web port open?  (Let's just use TCP ports 80, 443, and 8080)
Please enter your answer or press h for a hint:
```

41. Type `14372`

```
That's correct!
We used this as a solution:
grep -E "(80|443|8080)/open" bigscan.gnmap | wc -l
Using "-E" tells grep we"re giving it a regular expression (regex).  In this case, that regex
says, "I want lines that have 8080/open, 443/open, or 80/open."
If you want to be MORE correct, you might use "(\s8080|\s443|\s80)/open" to ensure you don't snag
ports like 50080, but there weren't any in this file.
You have 2 challenges left.
```

42. Type ``echo $((`grep Up bigscan.gnmap | wc -l` - `grep Ports bigscan.gnmap | wc -l`))``

```
402
```

43. Type `quizme`

```
How many hosts with status Up have no (detected) open TCP ports?
Please enter your answer or press h for a hint:
```

44. Type `402`

```
That's correct!
We used this as a solution:
echo $((`grep Up bigscan.gnmap | wc -l` - `grep Ports bigscan.gnmap | wc -l`))
Our solution is a little fancy, but the crux is this: use one grep|wc command to count how many
hosts are "Up", and use another to count how many have "Ports" open.
You have 1 challenge left.
```

45. Type ``echo $((1000 - `grep -oE "closed \([0-9][0-9][0-9]" bigscan.gnmap | cut -d"(" -f 2 | sort | head -n 1`))``

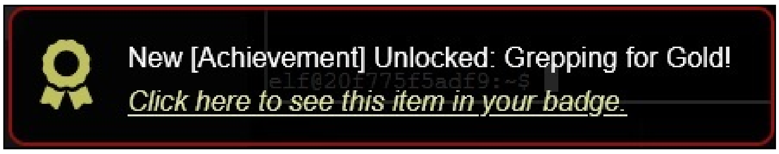
```
12
```

46. Type `quizme`

```
What's the greatest number of TCP ports any one host has open?
Please enter your answer or press h for a hint:
```

47. Type `12`

```
That's correct!
We used this as a solution:
grep -E "(open.*){12,}" bigscan.gnmap | wc -l && grep -E "(open.*){13,}" bigscan.gnmap | wc -l
In our solution, we count how many lines have "open" in them a number of times.  We get a few for
12 and none for 13.
One crafty tester employed the mighty powers of awk like this:
awk 'BEGIN {print}{print gsub(/open/,"") ""}' bigscan.gnmap | sort -nr | head -1
You've done it!
```



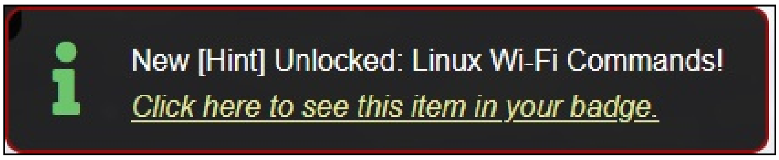
New [Achievement] Unlocked: Grepping for Gold!

Click here to see this item in your badge.

48. Click the `Close` button

49. Click to talk to `Greasy GopherGuts`

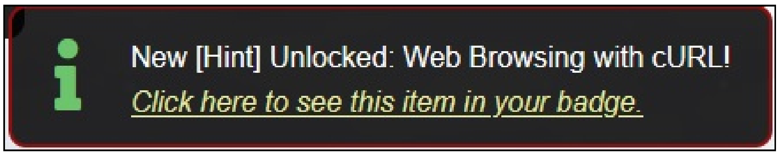
```
Grack. Ungh. ... Oh!

You really did it?

Well, OK then. Here's what I know about the wifi here.

Scanning for Wi-Fi networks with iwlist will be location-dependent. You may need to move around
the North Pole and keep scanning to identify a Wi-Fi network.

Wireless in Linux is supported by many tools, but iwlist and iwconfig are commonly used at the
command line.
```



New [Hint] Unlocked: Linux Wi-Fi Commands!
Click here to see this item in your badge.

50. Click to talk to `Greasy GopherGuts`

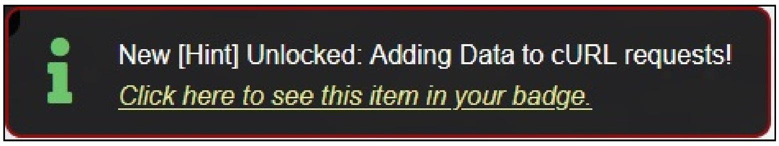
```
By default, curl makes an HTTP GET request. You can add --request POST as a command line argument
to make an HTTP POST request.
```



New [Hint] Unlocked: Web Browsing with cURL!
Click here to see this item in your badge.

51. Click to talk to `Greasy GopherGuts`

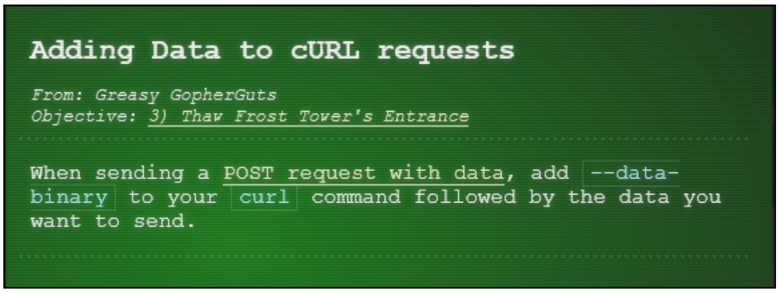
```
When sending HTTP POST, add --data-binary followed by the data you want to send as the POST body.
```



New [Hint] Unlocked: Adding Data to cURL requests!
Click here to see this item in your badge.

52. Click the `i` (Hints) icon

53. Click `Adding Data to cURL requests`

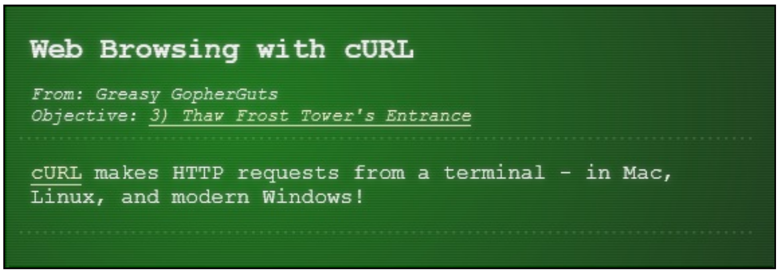


Adding Data to cURL requests

From: Greasy GopherGuts
Objective: 3) Thaw Frost Tower's Entrance

When sending a POST request with data, add `--data-binary` to your `curl` command followed by the data you want to send.

54. Click `Web Browsing with cURL`

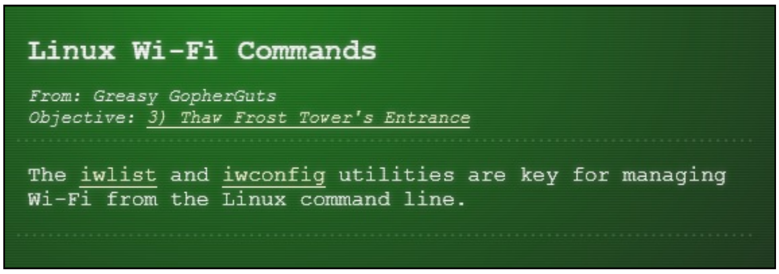


Web Browsing with cURL

From: Greasy GopherGuts
Objective: 3) Thaw Frost Tower's Entrance

cURL makes HTTP requests from a terminal - in Mac, Linux, and modern Windows!

55. Click `Linux Wi-Fi Commands`



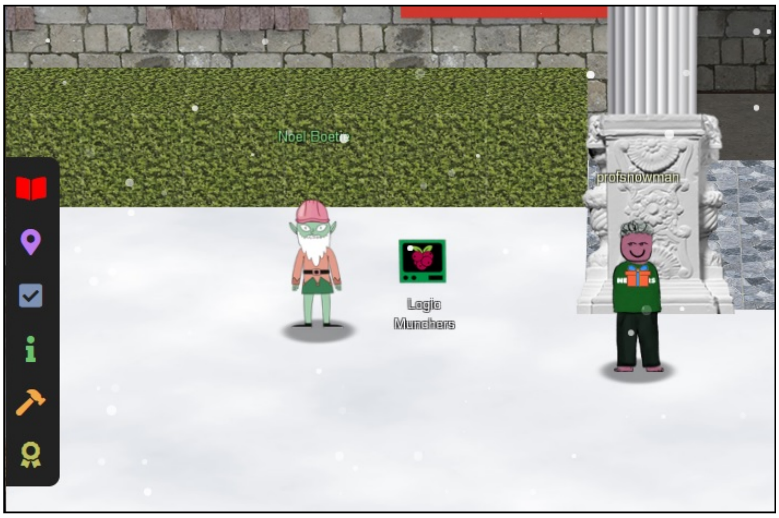
Linux Wi-Fi Commands

From: Greasy GopherGuts
Objective: 3) Thaw Frost Tower's Entrance

The iwlist and iwconfig utilities are key for managing Wi-Fi from the Linux command line.

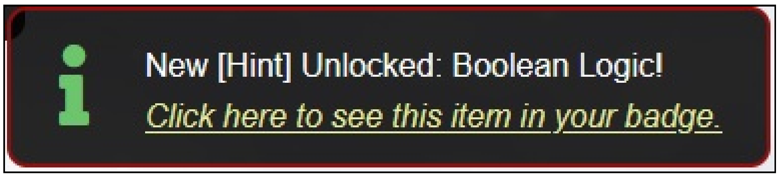
56. Click `[Exit]`

57. Move `Left`



58. Click to talk to `Noel Boetie`

```
Hello there! Noel Boetie here. We’re all so glad to have you attend KringleCon IV and work on the
Holiday Hack Challenge!

I'm just hanging out here by the Logic Munchers game.

You know… logic: that thing that seems to be in short supply at the tower on the other side of
the North Pole?

Oh, I'm sorry. That wasn't terribly kind, but those frosty souls do confuse me...

Anyway, I’m working my way through this Logic Munchers game.

A lot of it comes down to understanding boolean logic, like True And False is False, but True And
True is True.
```

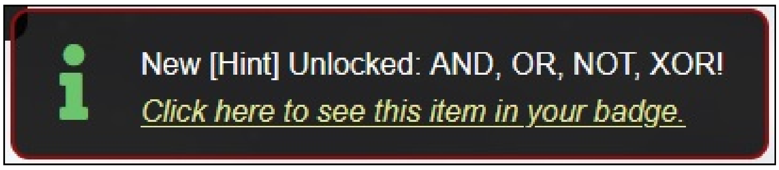


New [Hint] Unlocked: Boolean Logic!

Click here to see this item in your badge.

59. Click to talk to `Noel Boetie`

```
It can get a tad complex in the later levels.
```



New [Hint] Unlocked: AND, OR, NOT, XOR!

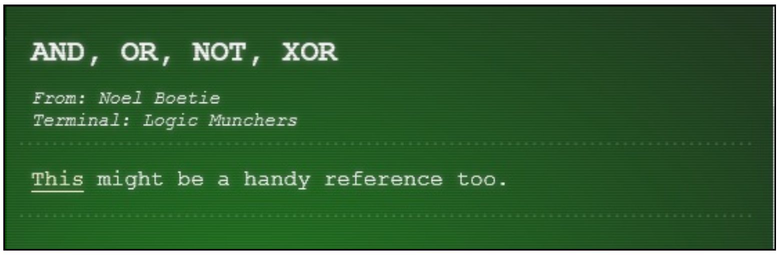
Click here to see this item in your badge.

60. Click to talk to `Noel Boetie`

```
I need some help, though. If you can show me how to complete a stage in Potpourri at the
Intermediate (Stage 3) or higher, I’ll give you some hints for how to find vulnerabilities.

Specifically, I’ll give you some tips in finding flaws in some of the web applications I’ve heard
about here at the North Pole, especially those associated with slot machines!
```

61. Click the `i` (Hints) icon

62. Click `AND, OR, NOT, XOR`

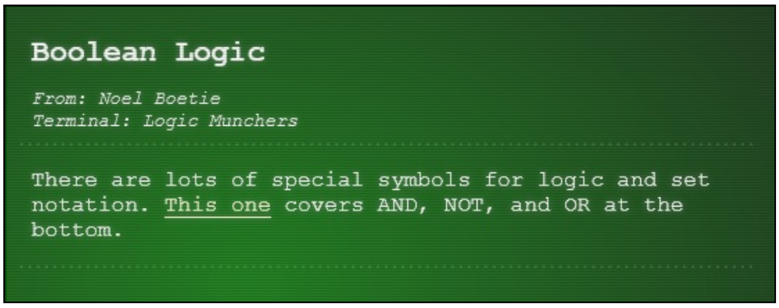


AND, OR, NOT, XOR

From: Noel Boetie
Terminal: Logic Munchers

This might be a handy reference too.

63. Click `Boolean Logic`



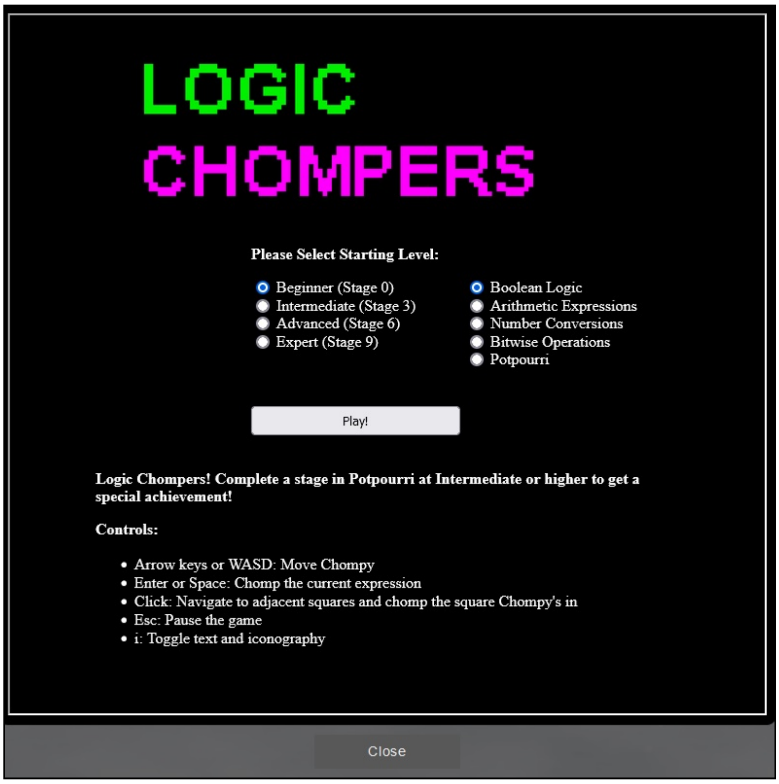
Boolean Logic

From: Noel Boetie
Terminal: Logic Munchers

There are lots of special symbols for logic and set notation. This one covers AND, NOT, and OR at the bottom.

64. Click `[Exit]`

65. Click `Logic Munchers` Cranberry Pi terminal



Please Select Starting Level:

● Beginner (Stage 0)	● Boolean Logic
○ Intermediate (Stage 3)	○ Arithmetic Expressions
○ Advanced (Stage 6)	○ Number Conversions
○ Expert (Stage 9)	○ Bitwise Operations
	○ Potpourri

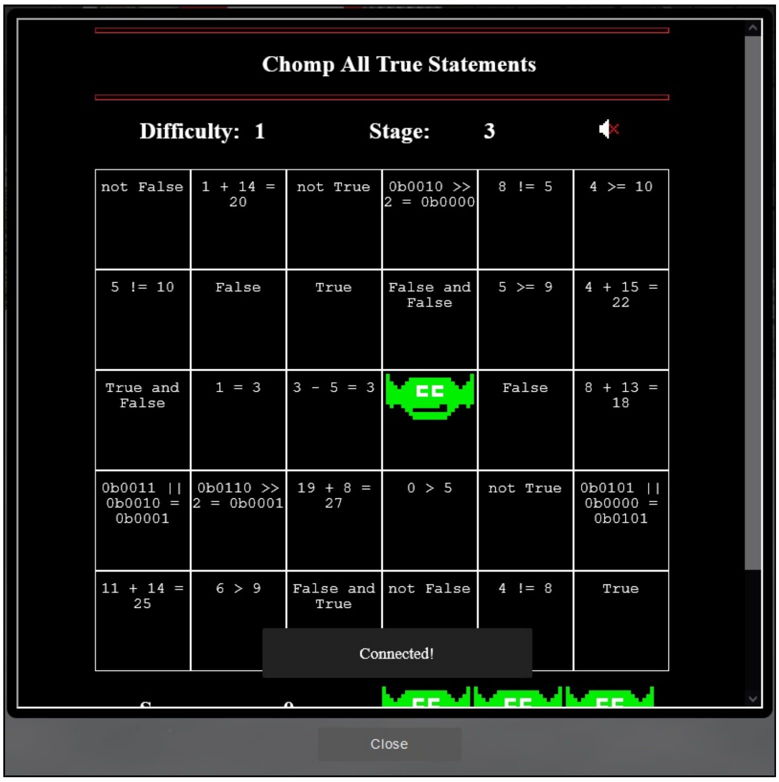
Logic Chompers! Complete a stage in Potpourri at Intermediate or higher to get a special achievement!

Controls:

- Arrow keys or WASD: Move Chompy
- Enter or Space: Chomp the current expression
- Click: Navigate to adjacent squares and chomp the square Chompy's in
- Esc: Pause the game
- i: Toggle text and iconography

66. Click `Intermediate (Stage 3)` and `Potpourri`

67. Click `Play!` button



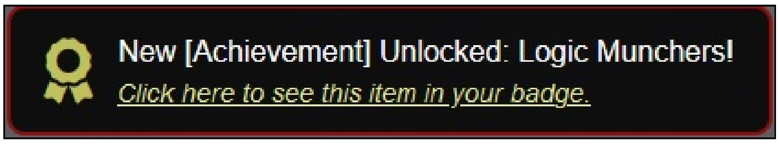
Chomp All True Statements

Difficulty: 1 Stage: 3

not False	1 + 14 = 20	not True	0b0010 >> 2 = 0b0000	8 != 5	4 >= 10
5 != 10	False	True	False and False	5 >= 9	4 + 15 = 22
True and False	1 = 3	3 - 5 = 3		False	8 + 13 = 18
0b0011 || 0b0010 = 0b0001	0b0110 >> 2 = 0b0001	19 + 8 = 27	0 > 5	not True	0b0101 || 0b0000 = 0b0101
11 + 14 = 25	6 > 9	False and True	not False	4 != 8	True

Connected!

68. Press `Space` or `Enter` to chomp the True squares



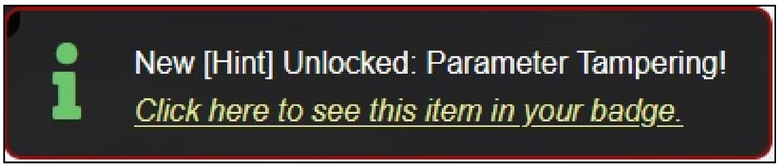
New [Achievement] Unlocked: Logic Munchers!

Click here to see this item in your badge.

69. Click the `Close` button

70. Click to talk to `Noel Boetie`

```
Wow - amazing score! Great work!

So hey, those slot machines. It seems that in his haste, Jack bought some terrible hardware.

It seems they're susceptible to parameter tampering.
```

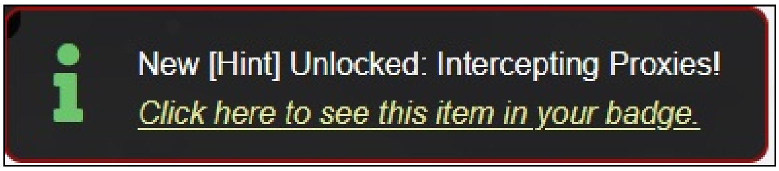


New [Hint] Unlocked: Parameter Tampering!

Click here to see this item in your badge.

71. Click to talk to Noel Boetie

```
You can modify web request parameters with an intercepting proxy or tools built into Firefox.
```

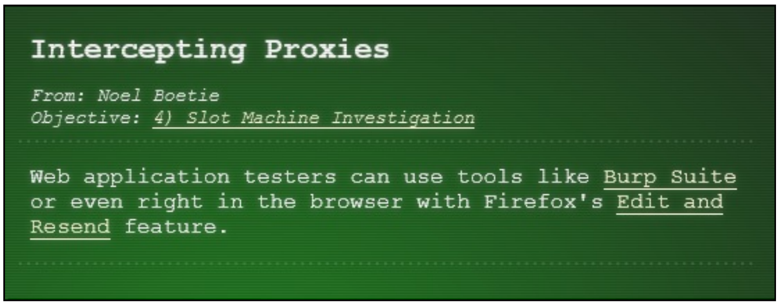


New [Hint] Unlocked: Intercepting Proxies!

Click here to see this item in your badge.

72. Click the i (Hints) icon

73. Click Intercepting Proxies



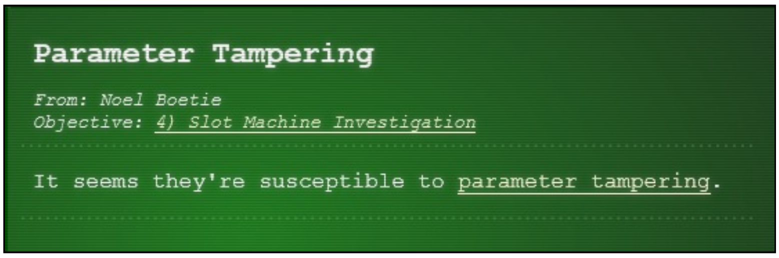
Intercepting Proxies

From: Noel Boetie

Objective: 4) Slot Machine Investigation

Web application testers can use tools like Burp Suite or even right in the browser with Firefox's Edit and Resend feature.

74. Click Parameter Tampering



Parameter Tampering

From: Noel Boetie

Objective: 4) Slot Machine Investigation

It seems they're susceptible to parameter tampering.

75. Click [Exit]

76. Move Up inside the Castle