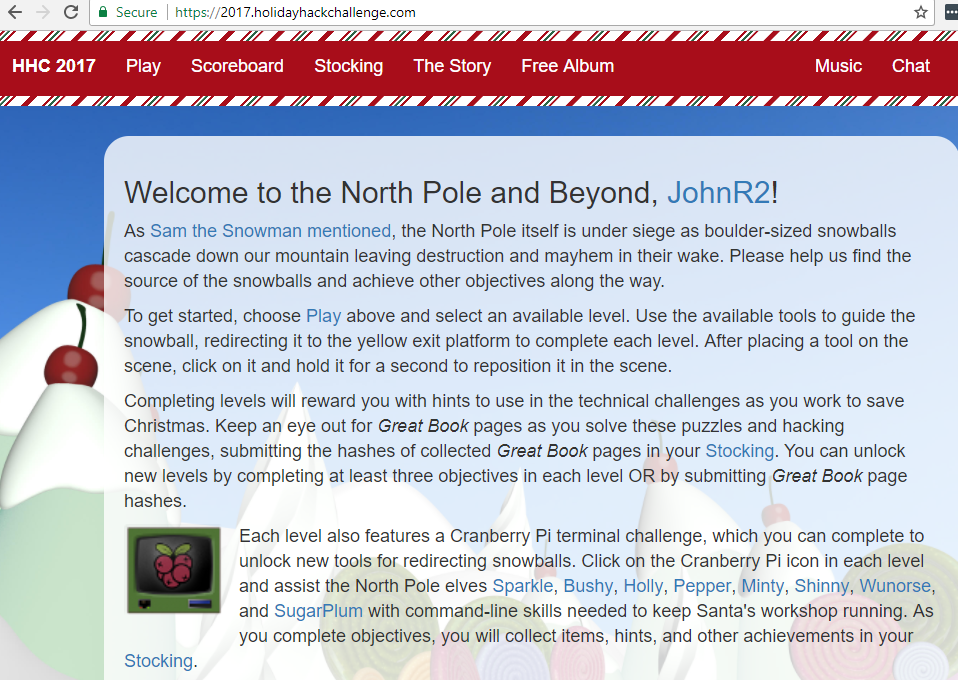
# Homework Assignment: Winter Wonderland Linux Challenge, or,

Linux Command Hijacking Terminal Challenge

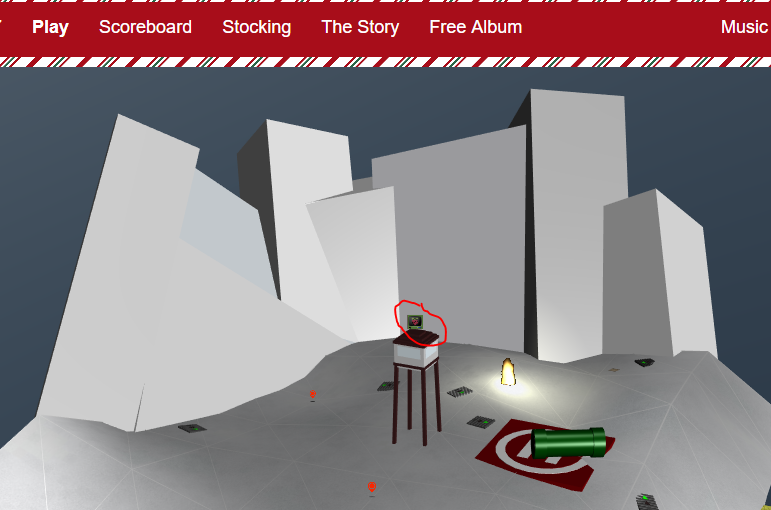
The key lesson from this assignment is, “What is the $PATH environment variable and what does it do?”

Visit the site <https://holidayhackchallenge.com/2017/>. After reading about the challenge, select “North Pole and Beyond” to go to the challenge site, <https://2017.holidayhackchallenge.com/>.

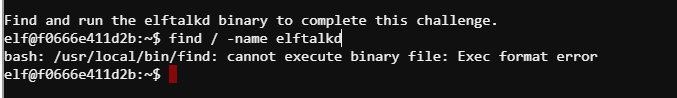
Register a new account, and log in. You should see this page: 

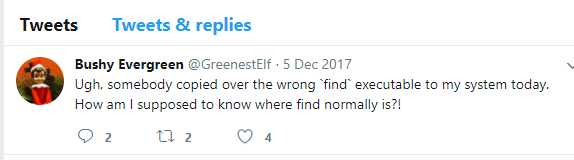
The links at the bottom, Sparkle, Bushy, etc., take you to Elf Twitter sites that have clues about the Linux Terminal Challenges.

To access the challenges, select Play. You should see this. 

The first Linux terminal challenge we will do is Winter Wonder Landing at the bottom. You don’t need to play the snowball game. Just click on the terminal icon that is on top of the box. 

The terminal should appear. `

The problem here is that the “find” command is not easilly accessible. 

Bushy’s tweet is a clue. 

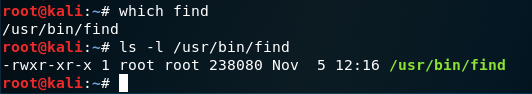
The key part is, “How am I supposed to know where find normally is?!” The linux terminal is based on Ubuntu. Kali is also based on Ubuntu. Hmmm. If you can answer Bushy’s question you can solve the challenge.

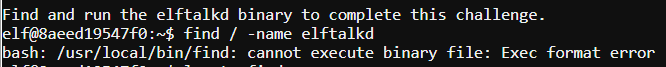
# To hand in:

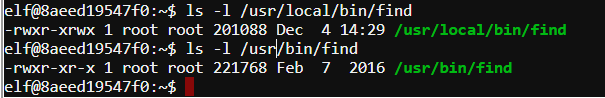
1. The command you used to find elftalkd, and the command you used to start efltalkd.
2. When the terminal shows up in your stocking, you’ll see that it is called the Linux command hijacking terminal challenge.
   1. Look at the path that the terminal uses.
   2. Compare the paths to the bogus version of find, the real version of find, and the path from step a.
   3. Why is this challenge called Linux command hijacking, and how did it work?

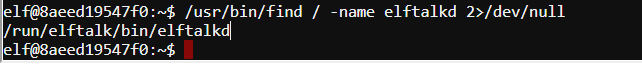
# Solution

## Method 1

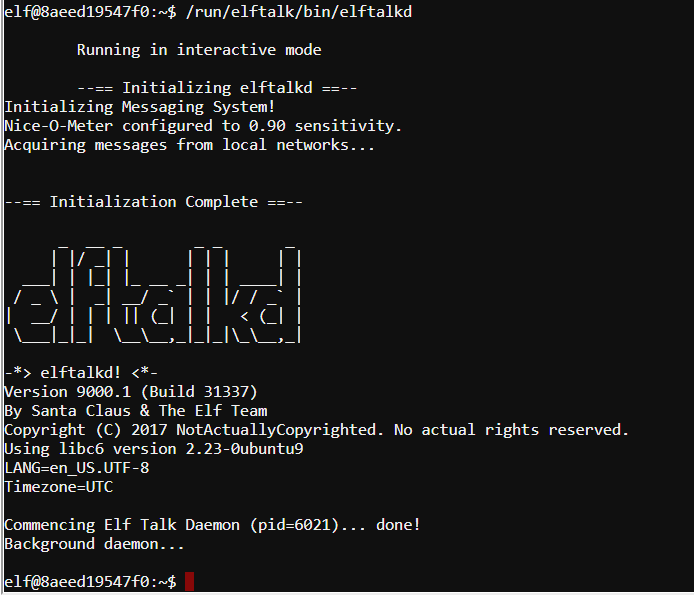
A look at an Ubuntu based VM shows that find is usually located in /usr/bin/.

However, the command that runs in the terminal challenge is /usr/local/bin/find. 

When we look at the two directories on the terminal, we find the find executable in both places. 

Let’s try the other find, in /usr/bin/find. 

The answer to the first part of question 1 is, /usr/bin/find / -name elftalkd.



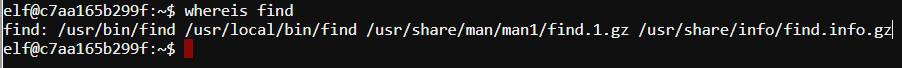
The answer to the second part of question 1 is, /run/elftalk/bin/elftalkd.

The path that the terminal uses to find executables shows the order in which terminal searches directories. 

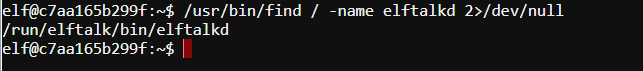
So,  
Path /usr/local/sbin /usr/local/bin /usr/sbin /usr/bin  
bogus find located here  
real find located here

The answer to question 2 is, someone hijacked the find command by putting a bogus copy of find (or a file named find) in a directory that is closer to the beginning of the path than the real find.

## Method 2

There is a command called whereis that can help us. 

There are two files named find. The one that doesn’t work is /usr/local/bin/find. When we try /usr/bin/find, it does work.



Note: The elf user does not have root access, so find generates errors when it comes across files that the elf user cannot access. The redirection, >2/dev/null, discards the errors so they don’t crowd the screen.

