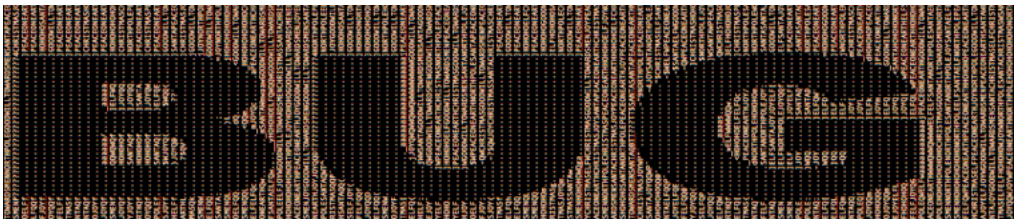
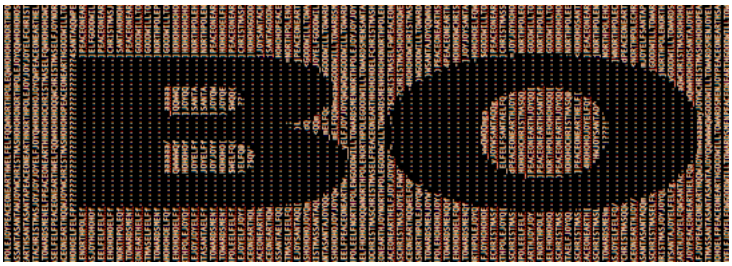
SANS Holiday Hack Challenge 2016 Write-up
Blake Irwin
1/4/17

This is the first year that I have fully participated in the SANS Holiday Hack Challenge. I really appreciate the awesome work that the Counter Hack team put into making such a great challenge. I was unable to fully solve the challenge, but had a blast doing it and learned a lot of new stuff that have already helped me at my job.

I began the challenge by reading through the storyline then jumping into the 8-bit world to begin exploring. Upon entering I found the business card left by Santa. The card led me to Santa's Twitter and Instagram accounts. To decipher the secret message in the tweets, I copied out all the tweets into a text editor and parsed out all data other than the tweets. I'm sure there are better ways to do this, but this worked for me. Once formatted in my text editor, vim, I was able to see the secret message in ASCII art. The secret message is "BUG BOUNTY".

1) What is the secret message in Santa's tweets?
BUG BOUNTY





I then moved onto the Instagram account. Closely analyzing the first photo, I found an nmap scan report for www.northpolewonderland.com on the desk along with a file name SantaGram_v4.2.zip on the monitor. I put these 2 items together and was able to download the zip file from Santa's website using this URL: www.northpolewonderland.com/SantaGram_v4.2.zip.

After downloading the file, I unzipped the file with the password “bugbounty”. This revealed an APK file.

2) What is inside the ZIP file distributed by Santa's team?
APK File

Then I used apktool to decode the app. Running strings against all output apktool and grepping for password and looking before and after 10 lines in order to find credentials I found the following output:

```
    invoke-direct {v0}, Lorg/json/JSONObject;-><init>()V
    :try_start_0
    const-string v1, "username"
    const-string v2, "guest"
    invoke-virtual {v0, v1, v2}, Lorg/json/JSONObject;-
>put(Ljava/lang/String;Ljava/lang/Object;)Lorg/json/JSONObject;
    const-string v1, "password"
    const-string v2, "busyreindeer78"
```

3) What username and password are embedded in the APK file?
guest / busyreindeer78

I then searched through the decoded and unzipped apk directory for “*.mp3” and found **discombobulatedaudio1.mp3**. The audio was unrecognizable.

```
find SantaGram/ -iname "*.mp3"
SantaGram/SantaGram_4.2/res/raw/discombobulatedaudio1.mp3
```

4) What is the name of the audible component (audio file) in the SantaGram APK file?
discombobulatedaudio1.mp3

I walked around the North Pole and found all 5 pieces of the Cranberry Pi and presented to Holly Evergreen. She provided me with an image to download and asked for the password. I mounted the image using fdisk and mount. I then extracted the hash for the cranpi account from /etc/shadow/. I copied the entry for cranpi into a text file and ran through john against the RockYou wordlist to crack the password.

```
# john --format=sha512crypt  --wordlist=~/Downloads/rockyou.txt cranpi-hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
yummycookies     (cranpi)
1g 0:00:11:13 DONE (2016-12-12 21:23) 0.001485g/s 674.7p/s 674.7c/s 674.7C/s
yves69..yuly1
Use the "--show" option to display all of the cracked passwords reliably
Session completed

# john --show cranpi-hash
cranpi:yummycookies:17140:0:99999:7:::
```

5) What is the password for the "cranpi" account on the Cranberry Pi system?
yummycookies

6) How did you open each terminal door and where had the villain imprisoned Santa?

Door to Elf House #2 – Room 2
To get the key to this door I ran strings against the pcap file as itchy to get part1 of the key. I guessed the 2nd half to determine the key was "**santaslittlehelper**".

```
scratchy@a6c58c5beb38:/$ sudo -u itchy strings /out.pcap
…
<input type="hidden" name="part1" value="santasli" />
…
```

Door to Santa's Office
To find the key, I ran a find command against the home directory and executed cat against each file and grepped for key. The key to this door is "**open_sesame**".

```
elf@99c473e7b32a:~$ find -type f -exec cat {} \; | grep key
key: open_sesame
```

Door to The Corridor
To open this door, I responded with the following text from WarGames. The key to this door is "**LOOK AT THE PRETTY LIGHTS**".

```
Hello.
I'm fine. How are you?
People sometimes make mistakes.
Love to. How about Global Thermonuclear War?
Later. Let's play Global Thermonuclear War.
```

2
Las Vegas Seattle

```
AWAITING FIRST STRIKE COMMAND
-----------------------------

PLEASE LIST PRIMARY TARGETS BY
CITY AND/OR COUNTRY NAME:

Las Vegas Seattle
CHOOSE A DIFFERENT CITY
Las Vegas
LAUNCH INITIATED, HERE'S THE KEY FOR YOUR TROUBLE:

LOOK AT THE PRETTY LIGHTS

Press Enter To Continue
```

Door to DFER

To open this door, I shot the Wumpus and received the key to the door: "**WUMPUS IS MISUNDERSTOOD**".

```
Care to play another game? (y-n) y
In the same cave? (y-n) y

You are in room 13 of the cave, and have 5 arrows left.
*whoosh* (I feel a draft from some pits).
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 2, 4, and 6.
Move or shoot? (m-s) s left
*thunk*  The arrow can't find a way from 13 to 0 and flys randomly
into room 6!

You are in room 13 of the cave, and have 4 arrows left.
*whoosh* (I feel a draft from some pits).
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 2, 4, and 6.
Move or shoot? (m-s) s wumpus
*thunk*  The arrow can't find a way from 13 to 0 and flys randomly
into room 4!
*thwock!* *groan* *crash*

A horrible roar fills the cave, and you realize, with a smile, that you
have slain the evil Wumpus and won the game!  You don't want to tarry for
long, however, because not only is the Wumpus famous, but the stench of
dead Wumpus is also quite well known, a stench plenty enough to slay the
mightiest adventurer at a single whiff!!

Passphrase:
WUMPUS IS MISUNDERSTOOD

Care to play another game? (y-n)
```

After entering the DFER, I found Santa Claus!

```
Workshop
DFER
<Santa Claus> - Well, hello there. You've rescued me! Thank you so much.
<Santa Claus> - I wish I could recall the circumstances that lead me to be imprisoned here in my very own Dungeon For Errant Reindeer (DFER). But, I seem to be suffering from short-term memory loss. It feels almost as though someone hit me over the head with a Christmas tree. I have no memory of what happened or who did that to me.
<Santa Claus> - But, this I do know. I wish I could stay here and properly thank you, my friend. But it is Christmas Eve and I MUST get all of these presents delivered before sunrise!
<Santa Claus> - I bid you a VERY MERRY CHRISTMAS… AND A HAPPY NEW YEAR!
<Santa Claus> - …
```

Train to 1978

Turned off brakes with BRAKEOFF command. Then found HELP opened in less. I used the ability for less to find and execute the ActivateTrain binary.

Brake Off:

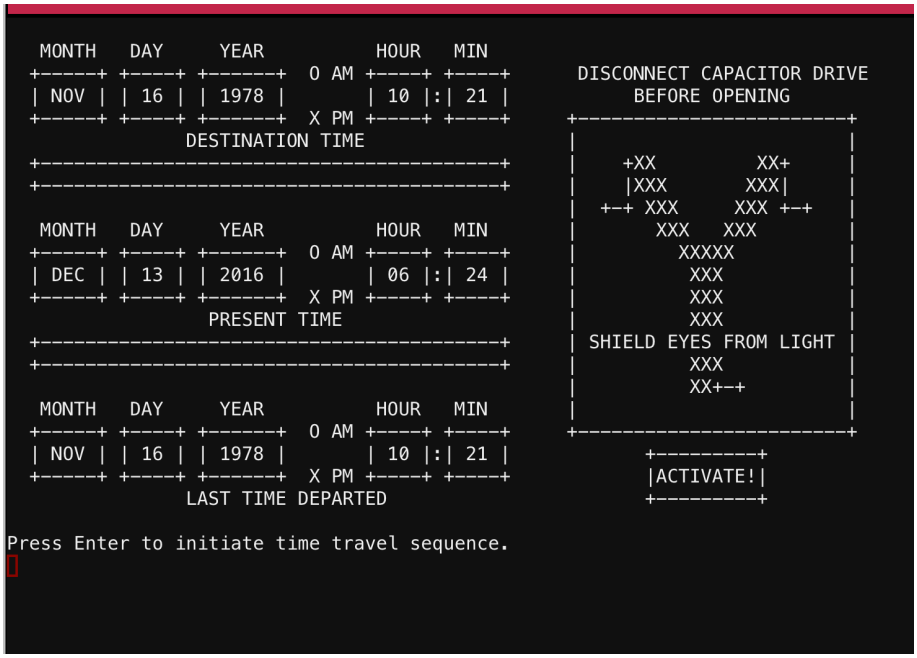
```
menu:main> BRAKEOFF

*******CAUTION*******
The brake has been released!
*******CAUTION*******
off
```

ActivateTrain executed from HELP menu:

```
1/4 cup lemon juice
1 dash ground cinnamon
!./ActivateTrain
```

Time Travel to 1978!



7) ONCE YOU GET APPROVAL OF GIVEN IN-SCOPE TARGET IP ADDRESSES FROM TOM HESSMAN AT THE NORTH POLE, ATTEMPT TO REMOTELY EXPLOIT EACH OF THE FOLLOWING TARGETS:

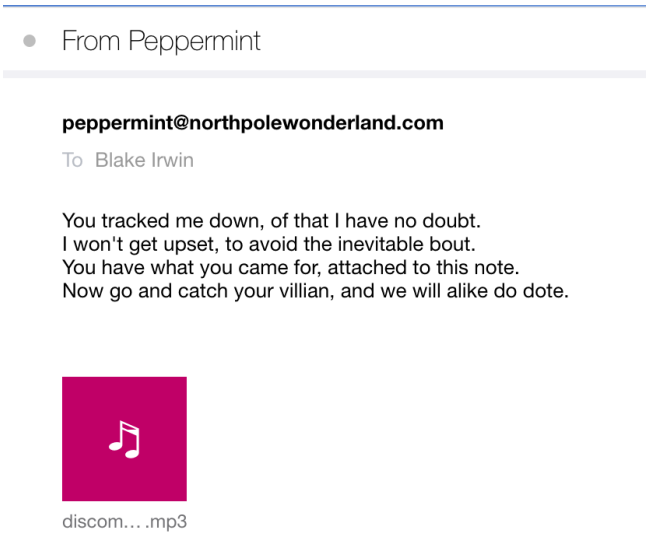
- **The Mobile Analytics Server (via credentialed login access)**
  - analytics.northpolewonderland.com
  - 104.198.252.157

To retrieve the MP3 file from the analytics server, I used the previously found credentials, guest / busyreindeer78 to login and downloaded the MP3 file via the MP3 tab.

- **The Dungeon Game**
  - dungeon.northpolewonderland.com
  - 35.184.47.139

To beat the dungeon, I retrieved the jewel-encrusted egg and provided it to the Elf at the North Pole. He provided me an email address to email. I emailed peppermint@northpolewonderland.com requesting the dungeon mp3 file.

>give egg to elf
The elf, satisfied with the trade says -
send email to **"peppermint@northpolewonderland.com"** for that which you seek.
The elf says - you have conquered this challenge - the game will now end.
Your score is 90 [total of 585 points], in 80 moves.
This gives you the rank of Novice Adventurer.



-
- **The Debug Server**
  - dev.northpolewonderland.com
  - 35.184.63.245

- **The Banner Ad Server**
  - ads.northpolewonderland.com
  - 104.198.221.240
- **The Uncaught Exception Handler Server**
  - ex.northpolewonderland.com
  - 104.154.196.33
- **The Mobile Analytics Server (post authentication)**
  - analytics.northpolewonderland.com
  - 104.198.252.157

The domains were found inside of the apk file, IPs resolved and confirmed by Tom Hessman.

This was as far as I was able to get. I retrieved 3/7 .mp3 files and rescued Santa.
Unfortunately the villain is still out there.