SANS Holiday Hack Challenge 2016

Part 1.

'Twas a month before Christmas, and all 'cross the webz,
Nothing was stirring, not e'en Brian Krebs.
Then from Ed's twitter there arose such a clamor,
Of a hacking challenge with prizes and glamor.

To my PC I rushed with serious haste,
For to win would need more than just copy and paste!
I started my VM's with caution and care,
To solve every challenge I knew would be there.

Josh and Jess Dosis met my arrival,
Their tale threated Christmas' very survival!
I viewed the scene and Santa's B-card,
And knew that this next step wasn't too hard.

Question 1. What is the Secret Message in Santa's Tweets?

With Python and Tweepy I scraped Santa's tweets,
(Which with my poor coding skills was quite a feat!)
On viewing the data, my head at an angle,
*I saw "**Bug Bounty**" and began to untangle,*
The clues left in images on Instagram,
To catch a criminal still on the lam.

I looked through the images,
And to my delight,
A URL in image one on the right.
The browser was uploading something of note,
A zip file named Santagram, and that's all he wrote.

Question 2. What is inside the ZIP file distributed by Santa's team?

A zip file you say? Most likely encrypted,
Time for John the Ripper, and a crack mostly scripted,
With wordlist so common, Rockyou by name,
An Android App file is next part of the game.

Part 2.

Question 3. What username and password are embedded in the APK file?

A user and password the Dosis kids seek,
So inside the app are the files I'll peek.
With "find" and "grep" and command line kung-fu
This user and password delivered to you.
The user is guest, his password much harder,
Busyreindeer78, that's question 3 for starter.

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

To find audio now is what we are after,
Inside this app, who was the drafter?
I'll bet to save space he used max compression,
An MP3 file let's look for this session.
*With find –name *.mp3 run from command line,*
Discombobulatedaudio1.mp3 showed up just fine.

Part 3.

Question 5. What is the password for the "cranpi" account on the Cranberry Pi system?

Assemble a "cran-pi" from pieces scattered
And give Holly a password, no doubt that it mattered!
Once more to Google again I did fly,
To see how to mount this here "cranberry-pi".
Once more on SANS website a solution was found
*'**sudo mount -v -o offset=70254592 -t ext4 cranbian.img SANS/cranbian**' …zounds!*
Now to crack passwords, again with dear John,
With 'unshadow' a new file did we spawn.
John --wordlist=rockyou.txt cranpi.txt was the command that we ran,
And the password yummycookie showed up in our scan!

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

To open each door is our tedious chore,
Each one a challenge, with elves keeping score.
The technical details, in truth are a bore,
*I'll skip that part here, I hope you aren't sore!**
We took a train, along tracks to the past,
To find Santa alone, but safe home at last!
In his dungeon for errant reindeer we found him,
But details of how he arrived there were quite dim!

Part 4.

Question 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)

The analytics server the easiest by far,
A user/password we already had, like a czar!
We entered credentials scored from SantaGram,
And another mp3 we had, thank you ma'am!

•The Dungeon Game

The dungeon game, required some guiding,
To find source code or cheats we knew which were hiding!
We found the GDT mode and read through the texts without fail,
And received attachment from Peppermint in our email!

•The Debug Server

The debug/dev server needed JSON, our clue,
So we poked and prodded until we were blue.
The results we got back had us baffled at first,
But I read the results the server disbursed.
What's this? It must be a flag through and through,
Mayhaps we need to set verbose to true?
I POSTed the following, 'cross the keys my hands flew,
{"date":"20160617000615+0000","udid":"1234567890123456789012345678901234567890ABCD","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","freemem":123455667, "verbose":true}
Indeed! We read the results with pure glee,
And downloaded debug-20161224235959-0.mp3!

•The Banner Ad Server

The Banner Ad server we knew from a tip,
Had Meteor running, but built with a slip.
Tim Medin had posted for finding rogue routes,
And a tamper monkey script to get hidden fruits!
We put it together and subscriptions we tampered,
And away from http://ads.northpolewonderland.com/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3
with our ill-gotten gains we scampered!

•The Uncaught Exception Handler Server

The EX server challenge we thought was quite shrewd,
A new twist on PHP local file include?
Once again, to SANS pen test blog we did go,
Where techniques Jeff McJunkin did show.
A way to get source code from server in question,
Some research on JSON and our skills we did freshen.
With Burpsuite to show our POST and response,
A payload inside a field we'd ensconce.
When processed the server did not ignore,
And displayed the source code in Base-64!
There at the top of the code plain to see,
In webroot was discombobulated-audio-6-XyzE3N9YqKNH.mp3!

•The Mobile Analytics Server (post authentication)

Part 5.

Question 9. Who is the villain behind the nefarious plot?

I assembled the audio obtained from the servers
And listened closely, an attentive observer
To my surprise, a villain, it's true!
Is none but the time travel-ing Dr. Who!

Question 10. Why had the villain abducted Santa?

I prodded and probed and inquired a-plenty,
It almost resembled the game questions twenty.
The Dr. confessed to his crimes without shame,
Not a single bit of remorse he did feign.
A movie of Star Wars and Christmas did he,
Attempt to prevent it from coming to be.

Conclusion:

And that my dear friends is this year's Christmas tale,
How I saved the day without worry or fail.
I hope you enjoyed this year's write up with cheer,
As I wait for another challenge next year!

**For the sake of rhyme and sanity, steps taken to access the doors were not covered*
Email: ncoppersmith@hotmail.com Twitter: @zoomzoomdude
-Nathan Coppersmith