Search for: Search

Bryce Boe

The Adventures of a UCSB Computer Science Ph.D. Student

Defcon 19 Quals Forensics 100 and Forensics 300 Solution

5 June, 2011 (19:18) | General | By: Bryce Boe

For the third year, I competed with team Shellphish in the Defcon quals. We pulled through with some amazing points at the end to finish in **8th place**. My successful contributions, however, were really only with respect to Forensics 100 and 300. My write up for the following are below:

Forensics 100
The forensics 100 challenge indicated to find the key, and **provided a png file** that was 19025×1 in resolution. Immediately our team thought we could simply change the resolution to **25×761** and would be on to something. After working with the resulting image for sometime I finally thought about converting it to **761×25**. That was our first break through when we read some text along the lines of “ILoveMeSomesheepysheepies” followed by binary that includes capital ‘O’s in place of some of the ’0’s. After no success with different permutations of that message we incorporated an idea the other team members had about the blue offset pixels that occur at regular intervals. Our first attempt at wrapping the image at the blue pixel boundaries (every 450 pixels) **resulted in success**! The key “thankYouSirPleasemayIhaveAnother” appeared and worked. The following is my simple python solution for Forensics 100:

```
#!/usr/bin/env python
import sys, Image

def main():
    orig = Image.open('f100.png')
    img = Image.new('RGBA', (450, 43))
    img.putdata(orig.getdata())
    img.show()

if __name__ == '__main__':
    sys.exit(main())
```

Forensics 300
Forensics 300 was quite an interesting challenge. I don’t have the original file, nevertheless, one had to extract the initial file with a password to get a dmg containing a dump from an iphone. I came into the challenge a little late, after one of my teammates had gone through all the images, videos, and audio files looking for Waldo and ‘grep’ing for various relevant keywords. Further more, my teammates had previously used the **iPhoneTracker** on the consolidated.db file to see where the phone had been, however San Antonio didn’t prove to be very useful.

While the iPhoneTracker app seemed pretty cool, I wanted to programmatically see where the phone had been the most. Thus, after figuring out what was what with respect to the consolidated.db file I wrote a little python script to find the most visited places rounded to less precision to account for some variance. The top three results were the following where the first number represents the number of occurrences in that location, and the two numbers between the parenthesis represent the latitude and longitude respectfully.

- 30 (‘-77.846’, ’166.677’)
- 18 (’0.000’, ’0.000’)
- 10 (’36.106’, ‘-115.173’)

When I did a **google search for the coordinates -77.846 166.667** I knew immediately that it was no coincidence that I was centered in a small town in Antarctica. Unfortunately, Google maps doesn’t have a name for this location so I had to **revert to Bing** (for the first time ever) to figure out that this location is called Ross Island. From that point we simply attempted different “places” listed **Ross Island’s wikpiedia page** until “McMurdo Station” submitted successfully. Below is the script I used to find the coordinates from the **consolodated.db input file**:

```
#!/usr/bin/env python
import os, sys

def main():
    os.system('sqlite3 consolidated.db "select Latitude, Longitude '
              'from CellLocation;" > tmp')

    uniq = {}
    for line in open('tmp'):
        pos = tuple('%.3f' % float(x) for x in line.split('|')[:2])
        if pos in uniq:
            uniq[pos] += 1
        else:
            uniq[pos] = 1

    for pos, count in sorted(uniq.items(), key=lambda x:x[1]):
        print count, pos

if __name__ == '__main__':
    sys.exit(main())
```

You can find links to solutions to other Defcon 19 Quals challenges at the **VNSecurity site**.

Related Entries

- **UCSB's International Capture The Flag Competition 2010 Challenge 6: Fear The EAR**
- **Defcon 18 Quals Forensics 200 Write up**
- **Bye Bye Facebook: A Guide to Leaving Facebook**
- **iCTF09 – UCSB's International Capture the Flag Competition**
- **The Python Multiprocessing Queue and Large Objects**

Tags: hacking, python

« More on the Execution After Redirect Vulnerability

Comments

Comment from **another team**
Time 2011/06/05 at 8:28 PM

I probably spent half a day on forensics 300! I scanned the dmg for deleted files and found all sorts of interesting things (including lots of photos of bros), and we looked at the universities that most of the gps coords seemed to be grouped around, and someone took the average of all the coords, which pinpointed Sheep Island in alabama.
tooooo many red herrings.

Comment from **Bryce Boe**
Time 2011/06/05 at 8:45 PM

I know exactly how you feel. One of my teammates had worked on this for nearly 6 hours, before I jumped in. I too spent probably two hours before deciding to look at the coordinates as I did here. While forensic challenges are hard to write, the challenge writers really need to try to make it obvious when you've found the solution and not hide it amongst other potentially viable solutions.

Comment from **Roman**
Time 2011/06/05 at 9:27 PM

I spent quite a few hours on that too. Among my many wrong turns were:
checking all the text messages
checking all the maps
listening to all the ringtones
checking for email
find . -exec strings {} \; | grep -i treas
and of course consolidated.db. I took the hint of 'where the treasure is' to mean that

I should look at the final location in consolidated.db as determined by the timestamp. I burned a lot of time when I found that there were 108 rows in that db that shared the max timestamp in the db. So I spent a lot of time copy pasting lat/long coords into google maps looking for city names. This was the writeup I was really looking forward to, so thanks for sharing!!

Write a comment

Name:

E-mail:

URL:

Message:

Submit!

□ Notify me of followup comments via e-mail

Follow Me (bboe) on Twitter

Yes then maybe we can get some web based challenges. RT @gianlucaSB Maybe it's time for somebody else to take over defcon ctf... **2 hours ago**

Solution to Forensics 100 and 300 at: **http://goo.gl/YOWCu #quals #defcon #ddtek 3 hours ago**

My computer science education research career officially started today! **3 days ago**

.@**gianlucaSB** Wait, I know the answer that @**Zardus** would say! "Your momma!" **3 days ago**

. @**gianlucaSB** kind of hits home a bit doesn't it? **http://ti.me/imbDZe 1 week ago**

Recent Comments

Roman on **Defcon 19 Quals Forensics 100 and Forensics 300 Solution**

Bryce Boe on **Defcon 19 Quals Forensics 100 and Forensics 300 Solution**

another team on **Defcon 19 Quals Forensics 100 and Forensics 300 Solution**

little miss savage on **Random Lines from a File**

И еще немного про уязвимости авторизации « Безопасность веб-приложений: просто о сложном on **UCSB’s International Capture The Flag Competition 2010 Challenge 6: Fear The EAR**

jov on **How do I end it?**

VirusTotal plugin for IDA Pro | Hex Blog on **Submitting Binaries to VirusTotal**

pyc/weblog» Blog Archive » vector intersection on **Line Segment Intersection Algorithm**

Deweloperka w piątek | Wiadomości o technologiach IT on **Submitting Binaries to VirusTotal**

Hudson on **Dynamic Programming – Coin Change Problem in Python**

Blogs

Regular Expression – Jonathan Kupferman's Blog

My Sites

Bryce Boe @ UCSB CS

Hash House Harriers of Sant'o Barbara

priceTrackr

Tags

acm C EAR facebook family google hacking interview question javascript mac priceTrackr python recreation s3 security teaching unix commands Wednesday WTF

Subscribe to feed

Powered by WordPress | Theme design by Andreas Viklund