Daniel Roh

CMSC 491/791 Active Cyber Defense HW 2

Instructions

- Tonight, we hosted a Capture The Flag competition with different challenges of varying point values.
- For this assignment, you must solve at least 250 points worth of CTF challenges.
- Choose at least 250 points worth of challenges that you solved during the CTF. Your homework submission must include the following for each challenge:
    - The name of the challenge
    - How many points the challenge was worth
    - The challenge's flag
    - A writeup, approximately 1 paragraph in length, describing how you solved the challenge
- Write-ups are fun to do after CTFs and allow you to further explain what the challenge was about and what you learned. Here are a couple of examples of good write-ups:
    - https://rpis.ec/blog/tokyowesterns-2019-gnote/
    - https://ass.is/2019-03-27/dawgctf2019-where-am-i/
    - https://zackorndorff.com/2018/11/13/csaw-ctf-finals-2018-wic-wac-woe-1-writeup/#more-125
- Although the CTF was team-based, all homework submissions must be done individually and should only include the problems that you solved.

Due: September 18, 2019 at 7:00pm

Solved Flags

Name: Days Untill Area 51 Raid: 3
Points: 50
Flag: DawgCTF{33_24_104_30}
An image was given which gave out a "super good" plan for attacking area 51. The flag was found by first taking a look into the image's metadata which gave a hint on what the flag was "Flag format: DawgCTF{<degN>_<minN>_<degW>_<minW>}". From there, by looking back at the metadata, the geotagged information was conveniently given. From there it was just placing the numbers in the correct format to acquire the flag.

Name: Crypo 0
Points: 10
Flag: DawgCTF{T3stC0mpl3t3}
A short file with python code was given, in which the code returns a test message. In the comments, a way to return the flag was given in which one just needs to replace the message from "tst:hello" to "flg" to get the flag from the server.

Name: Emperor Bash
Points: 50
Flag: DawgCTF{1M_f33l1ng_1T}
For this challenge, the challenge prompted us to connect to a server via “nc ctf.notanexploit.club 8081”. Once connected, I was given a prompt where I needed to choose between entering “fe” or “ba”. By entering “ba”, the code caused the dump of the two differnt outputs, in which one included the flag, plus the code that was used for this challenge.

Name: Reversing 0
Points: 10
Flag: DawgCTF{it_0n3y_g3t$_hard3r_fr0m_h3r3}
For this challenge, a file was given. When attempting to open this file, it lead to an error in which the file could not be opened. By opening the file in an editor gave back a file with a lot of junk. However, by looking through the junk, a string with the flag was found.

Name: Reversing 1
Points: 40
Flag: DawgCTF{5tr1ng_m3_al0ng}
For this challenge, another file was given. Once again the file was unable to be opened. So the file was opened in an editor which once again resulted in a lot of junk being shown. After shifting through the junk, a string that showed “enter encoded flag” was found with what appears to be an encoded flag “TqmwSJV{5jh1dw_c3_qb0dw}”. After looking through some common ciphers to figure out what cipher may have been used. Eventually, I stopped at a shift cipher as I felt given the difficulty of this challenge, it may be the cipher that was used. Once finding a shift cipher decoder online, I placed the string in and messed around with the shift until a shift of 10 gave out the flag.

Name: Hash Browns
Points: 50
Flag: DawgCTF{S%2a9l}
For this challenge, a text file was given. In this text file was a bunch of encoded strings using various encryption algorithms. After painfully taking each string and finding a convenient decrypter for each algorithm it was seen that each string was a letter for the flag. After decrypting each string, the flag was found

Name: Pretty Basic
Points: 50
Flag: DawgCTF{r4m1x}
For this challenge, another text file was given. However, there was a bunch of numbers which appeared to be binary values. After thinking a bit about these numbers, it came to realisation that at the end of each of these sets of numbers were “b” and a number. This was giving a hint that these numbers where numbers encoded into various bases from 2 to 15. After decoding the bases to decimal (~~by hand~~, jk aint nobody got time for that). A set of numbers was given, in

which was quickly realised some ascii or unicode values. Once consulting an ascii table, a garbage text was given. So after consulting a unicode table the flag was found.

Name: Wish I had more spare time to work on these more
Points: 0
Flag: N/A