**Binary Exploits**

* Shane and the binary files (Alex)
* Given: Given a zip file of java bytecodes
* Solution:
  + Decompiled one particular .class file which asked for input using (http://www.javadecompilers.com)
  + The class file did a comparator between a randomly generated string and user input, and printed out some text based on a char array
    - Solution was obfuscated
    - (System.out.println("" + arrayOfChar[39] + arrayOfChar[6] + arrayOfChar[14] + arrayOfChar[17] + arrayOfChar[11] + arrayOfChar[13] + arrayOfChar[10] + arrayOfChar[20] + arrayOfChar[0] + arrayOfChar[13] + arrayOfChar[10] + arrayOfChar[2] + arrayOfChar[6] + arrayOfChar[14] + arrayOfChar[25] + arrayOfChar[65] + arrayOfChar[63] + arrayOfChar[65] + arrayOfChar[36] + arrayOfChar[6] + arrayOfChar[20] + arrayOfChar[64] + arrayOfChar[11] + arrayOfChar[8] + arrayOfChar[65] + arrayOfChar[11] + arrayOfChar[2] + arrayOfChar[17] + arrayOfChar[19] + arrayOfChar[10] + arrayOfChar[65] + arrayOfChar[63] + arrayOfChar[65] + arrayOfChar[47] + arrayOfChar[19] + arrayOfChar[8] + arrayOfChar[65] + arrayOfChar[22] + arrayOfChar[0] + arrayOfChar[13] + arrayOfChar[17] + arrayOfChar[65] + arrayOfChar[2] + arrayOfChar[25] + arrayOfChar[65] + arrayOfChar[13] + arrayOfChar[28] + arrayOfChar[32] + arrayOfChar[3] + arrayOfChar[45] + arrayOfChar[21] + arrayOfChar[25] + arrayOfChar[54] + arrayOfChar[7] + arrayOfChar[20] + arrayOfChar[28] + arrayOfChar[57] + arrayOfChar[48] + arrayOfChar[21] + arrayOfChar[32] + arrayOfChar[53] + arrayOfChar[53] + arrayOfChar[37] + arrayOfChar[0] + arrayOfChar[14]);
  + Moved the char array and above print statement into a new java function which outputted the flag
  + > Congratulations ! You're right ! The flag is aKMqGxs4duK7PxM33Bln

**Cryptography**

* Game of Fame (Alex)
* Given: p xasc. a zdmik qtng. yiy uist. easc os iye iq trmkbumk. gwv wolnrg kaqcs vi rlr.
  + Hint1: The seven star-studded Pragyan walks into the hall of fame. Boom!
  + Hint2: Robert Sedgewick
* Solution:
  + Attempted numerous ciphers, including brute force frequency analysis
  + Determine the ciphertext was encoded using a Vigenere cipher, with key (pragyan)
  + Plaintext result: a game. a movie star. his wife. a cs textbook. the winner takes it all
  + Flag was Robert Sedgewick’s textbook, algorithms

**Forensics**

* Look Harder (Jason)
  + Given: treasuremap.png
  + Solution: Open the result in a picture editing program (paint in my case), fill in the “yellow spots” with black. Scan it using a QR code reader (it was obvious).
  + Flag:
* Interstellar (Zhenyang)
* Given: transmission.png
* Solution: python script: // it’s really easy. I guess the organization used the alpha value to encode the flag
  + from PIL import Image
  + Image.open("transmission.png").show()
* Flag: Cooper\_Brand

**Miscellaneous**

* Game Starts Here
  + Given: None
  + Solution: Type “pragyanctf{HelloWorld}”

**Reverse Engineering**

**Stenography**

* Star war (Zhenyang):
  + searched on github
  + link “https://github.com/jklm264/CTF-Write-ups/blob/master/Pragyan%20CTF”