CSAW CTF 2016 Quals: Clams_Dont_Dance

Category: Forensics

Points: 150

Solves: 238

Description: Find the clam and open it to find the pearl.

Write Up:

So we were given a file called out.img. I ran file on it to determine what the image was of.

I found out that it was a x86 boot sector

So I liked using binwalk during CSAW.

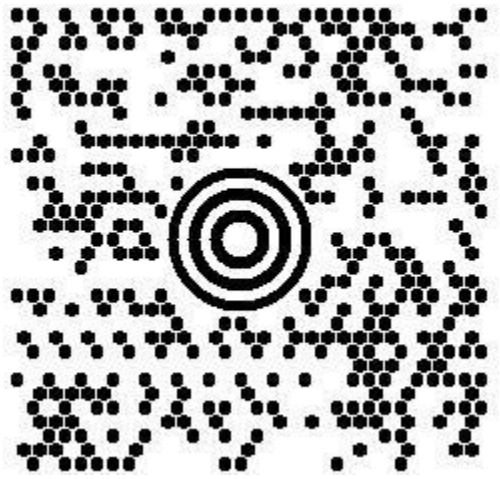
Binwalk is a pretty neat firmware analysis tool that is used for image analysis and extraction.

“binwalk out.img” shows that within the image there was a folder called ppt, an extension for Microsoft Power Point.

That folder was a bit interesting, so I typed in “binwalk -e out.img” to extract everything within the image into another folder.

My initial suspicion that the flag was in the xml file were unfounded as I couldn’t find anything there. After reading through the xml files I decided to check the media folder.

Within the media folder was a file called image0.gif which is a MaxiCode.



The MaxiCode will reveal the flag.

Flag

flag{TH1NK ABOUT 1T B1LL. 1F U D13D, WOULD ANY1 CARE??}