

FireEye Flare-On 2015 (1-5)

Jaime Geiger

whoami

- root
- I like C and assembly
 - Talk to me about those things
- I do CTFs
- I like helping people with programming



Shameless Plugs

- Get involved in CTF
- Get involved in RVAPT
- Come to RC3
- Keep coming to SPARSA
- Love what you do (security is awesome)



Flareon?



Flare-On!


- FireEye's yearly reverse engineering challenge!
- Fun
- <http://flare-on.com>



Challenge 1 - Simple XOR

- Windows Binary...
 - Let's take a look...
- EntryPoint is a good place to start
- We want "You are success"
- Byte by byte static xor key of 0x7d
 - Our input xor'ed and then compared with what's in the binary
- Where is our input? Where is the encoded key?
 - Look at ReadFile: 0x402158; encoded key is at our input minus 0x18

Challenge 2 - Bogus Instructions

- Find the encoder function
 - Find the length that the key needs to be (36 + \n)
 - Figure out where the encoded data is referenced (edi)
 - Identify operations that actually matter
 - Figure out the first character
 - Apply math - $((\text{byte} - (1 \ll (3 \& \text{count})) - 1) \wedge 199)$
 - Write script
 - Profit
- 

Challenge 3 - Let me take an Elfie


- What is this... Compiled python binary
- Google some strings
- Looks like pyinstaller
- Google pyinstaller extractor
- What is this?!
 - Come on. That's a big file.
 - Make python do the work for us
- It's easier to find than you think...



Challenge 4 - YouPecks

- Packed with UPX, IDA doesn't like it
 - UPX -d won't unpack it
- Let it unpack and then look around...
 - Base64, "4 + 4 =", and atoi
 - Look at atoi... has your input!
 - Hashes only 1 "byte" (0-255)
- Brute force the key
- `for /L %a in (0,1,255) do @youPecks.exe %a | findstr flare`

Challenge 5 - Custom Base64 Map

- Pcap
 - Look at the post requests! (grab that data to decode it)
 - Sender program
 - Run the program... key.txt
 - Create one with distinct input!
 - Look at where this data is going (xref "key.txt", ReadFile)
 - Two encoding stages
 - Stage 1: add static key
 - Stage 2: Custom base64 map
 - (Do this in reverse with the data from pcap to get the answer!)
- 

Challenge 6 - Android Application!

- Native ARM library (.so)
- Didn't get through this one :(



Da end

DA END

word.

