ACM NetSec

CTF Problems

November 9, 2017

Overview

Here are a list of problems we'll be tackling this session! They're divided into categories based on difficulty and this will give you insight into what California CTF will be like next year. We'll keep adding to this google doc throughout the quarter. Also, some of the links may seem sketch, but I tested them out and they're fine.

Beginner Problems

These problems are based on the slides from today's session and they have solutions online! All you need for these problems is the ability to read code and google. So, no prior experience required, just the ability to Google!

We'll mainly be working on pwnable.kr (http://www.pwnable.kr/)

Try out these questions first, everything else is probably much harder:

OverTheWire

- http://overthewire.org/wargames/bandit/
- Start out with bandit and work your way up!

Pwnable

- fd
    - File descriptors in Unix
- random
    - Hint: If what's generated isn't random, how can you figure out what is generated?
- cmd1
    - Hint: What Linux commands can you use? How can you make this command apply to a
- flag
    - GDB and unpackaging

Intermediate to Advanced Problems

Here are some more problems for people with prior CTF experience! Remember to poke one of the mentors if you get stuck at any step.

Pwnable

http://pwnable.kr

- tiny_easy
- otp
- simple login

Reverse Engineering Challenges

- https://challenges.re/

- https://pwnable.tw/challenge/
-

Resources

- CTF UCLA 2017's Beginner's Guide (tons of resources listed here):
  - tinyurl.com/ctfbeginnersguide
- GDB Guide:
  - https://beej.us/guide/bggdb/
- A bunch of video tutorials:
  - http://liveoverflow.com/binary_hacking/reverse_engineering.html
- objdump:
  - https://linux.die.net/man/1/objdump
- Slides from the previous sessions:
  - tinyurl.com/ctfslides1
  - tinyurl.com/ctfslides2
  - tinyurl.com/ctfslides3
- KITCTF's Guide
  - https://kitctf.de/learning/getting-started
- https://www.reddit.com/r/netsecstudents/comments/2wdkle/any_beginner_guides_for_ctf/
- Trail of Bits:
  - https://trailofbits.github.io/ctf/
- SSH tutorial for Windows users
  - https://support.suso.com/supki/SSH_Tutorial_for_Windows