Information Security Laboratory

CTF
Sang Kil Cha
Capture The Flag (CTF)

Capture the flag (CTF) is a traditional outdoor game where two teams each have a flag (or other marker) and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base.

- Wikipedia
CTF in Security

CTF = hacking competition

e.g., Def Con (started in 1993)
Two Types

• Jeopardy style
  – Problem solving
  – One-way
  – Easier to organize

• Attack-and-defense style
  – Dynamic and interactive
  – Difficult to organize
  – Few CTFs including Def Con final
Jeopardy

* Image from https://upload.wikimedia.org/wikipedia/commons/d/d8/Jeopardy_game_board.png
Def Con

* Image from http://farm4.static.flickr.com/3068/2751067339_67580e149a_d.jpg
Our CTF

• 2:30pm – 9pm, 5/31 @ N5 #2310

• Attack-and-defense style
  – Defense = Snort only (no S/W patch)

• Bring your laptop
• All the source code will be available
Space Allocation (2310)

Team 1

Team 2

Team 3

Team 4

Team 5

TAs

Door
Several Tips

• Use IRC, Slack, or similar for communication
• Prepare your attack scripts
• Study the network setup
• Study Snort, iptables, tcpdump, etc.
• Study how to use raw sockets
Write-Up Due

- Due: 23:59:59pm, 6/12
- Describe in a markdown file how you exploited a vulnerability
  - Create a separate file for each exploitation
  - Create a markdown file that has links to each description

- Include 3 things:
  - What was the attack vector?
  - What was the vulnerability?
  - How you exploit the vulnerability? (include your attack script as well)

- N.B. 30% of your grade will be determined by the group activity!
Question?