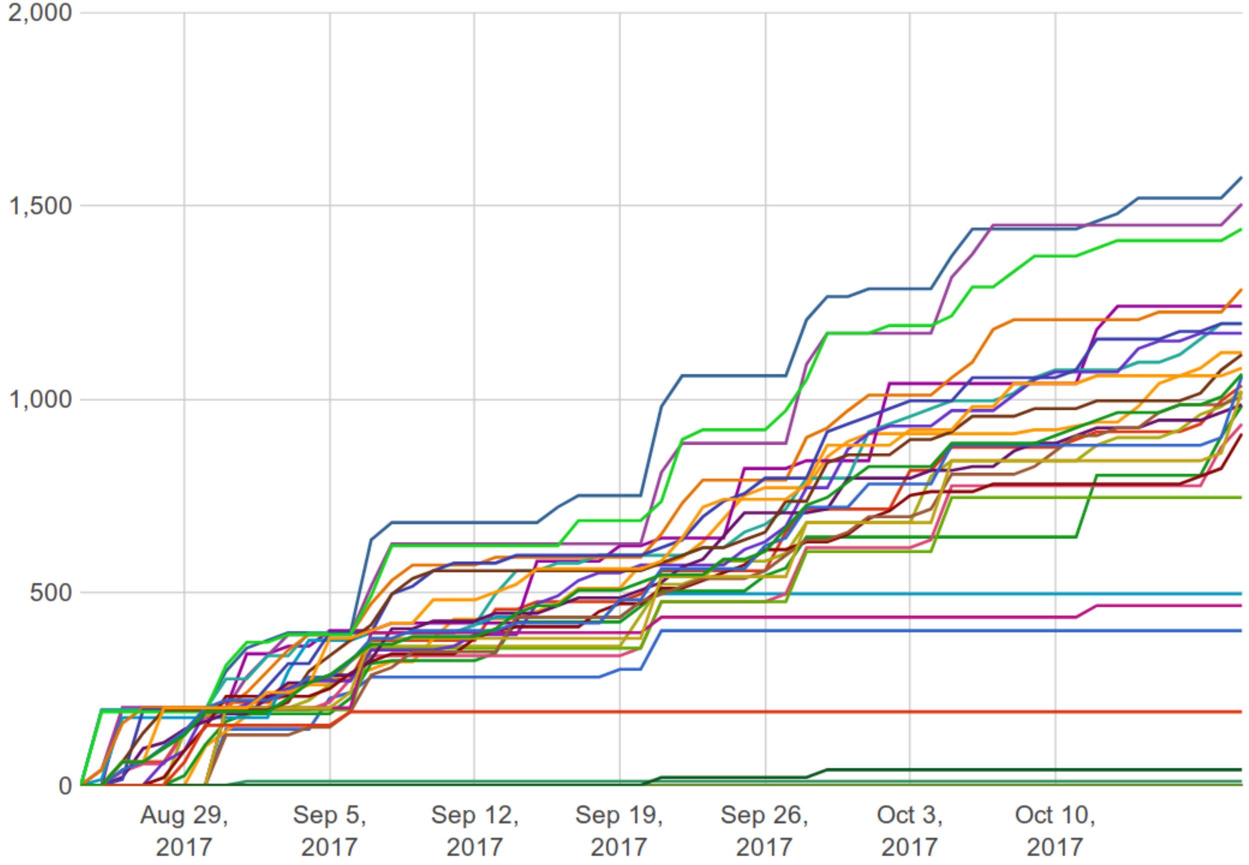
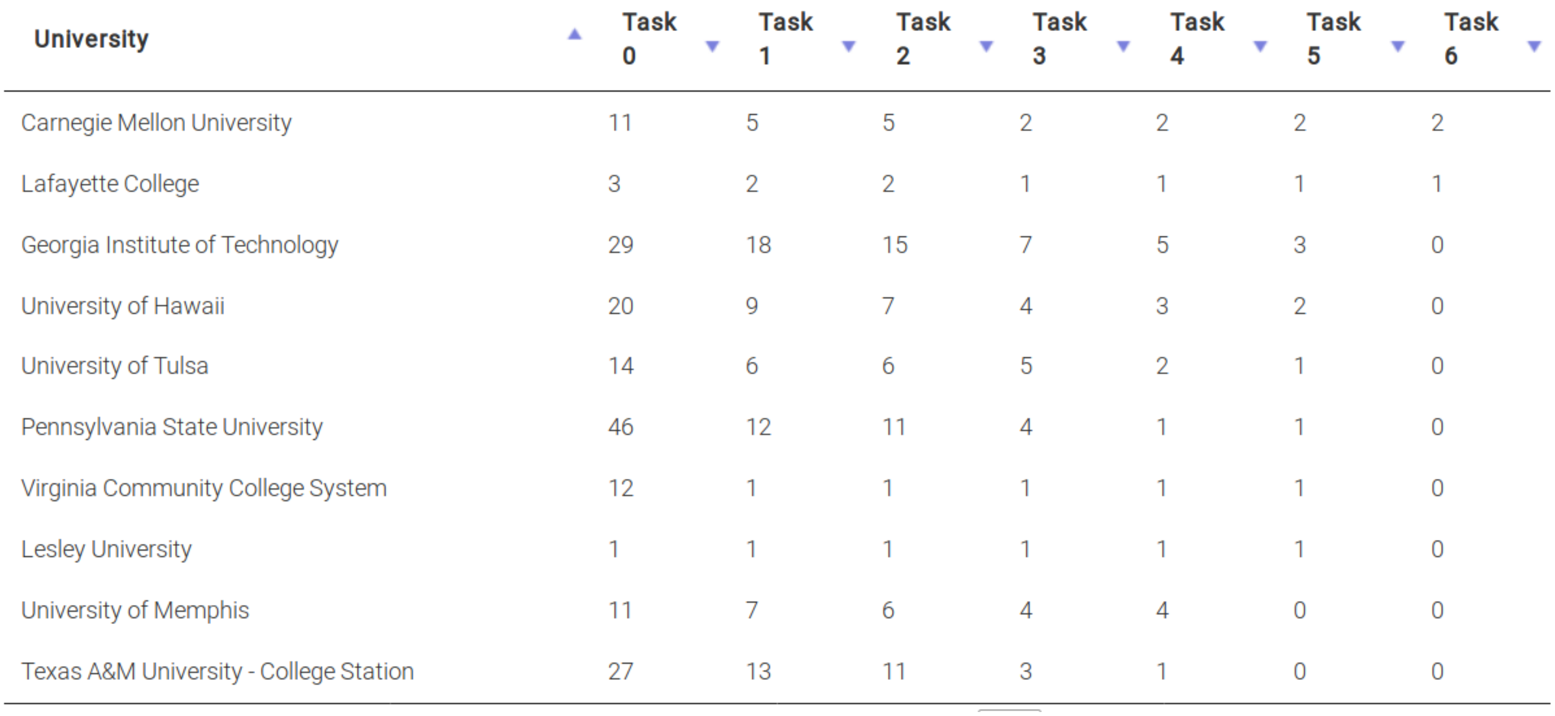
Lec08: Remote Exploit

Taesoo Kim

Scoreboard


2,000
1,500
1,000
500
0
Aug 29, 2017
Sep 5, 2017
Sep 12, 2017
Sep 19, 2017
Sep 26, 2017
Oct 3, 2017
Oct 10, 2017

NSA Codebreaker Challenges

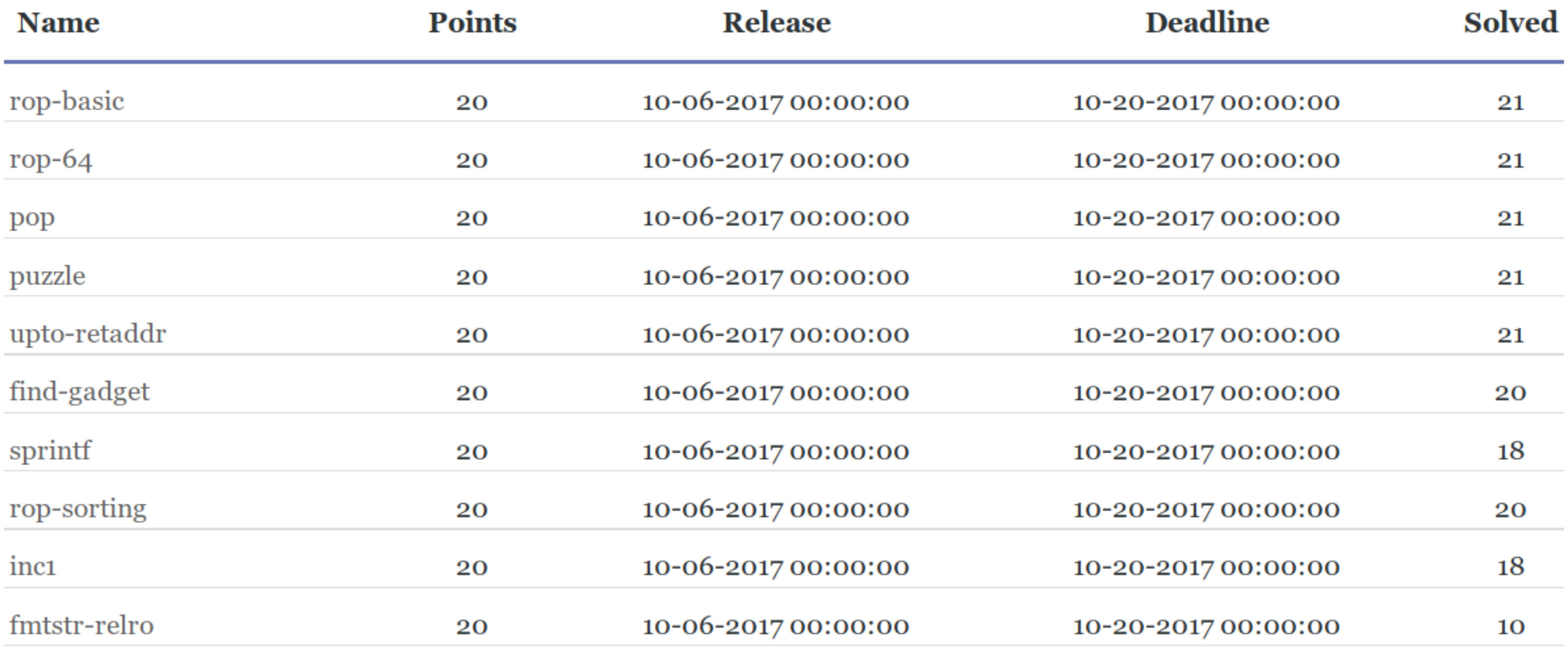


University	Task 0	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6
Carnegie Mellon University	11	5	5	2	2	2	2
Lafayette College	3	2	2	1	1	1	1
Georgia Institute of Technology	29	18	15	7	5	3	0
University of Hawaii	20	9	7	4	3	2	0
University of Tulsa	14	6	6	5	2	1	0
Pennsylvania State University	46	12	11	4	1	1	0
Virginia Community College System	12	1	1	1	1	1	0
Lesley University	1	1	1	1	1	1	0
University of Memphis	11	7	6	4	4	0	0
Texas A&M University - College Station	27	13	11	3	1	0	0

Administrivia

- Hacking day on Oct 27 (No class)!
- If you are interested in, check out CTF Events
- One local CTF game (on 11/04/2017): Hungry Hungry Hackers 2017
- Due: Lab08 is out and its due on Nov 2 (two weeks!)
- NSA Codebreaker Challenge → Due: Nov 30

Lab06: ROP



Name	Points	Release	Deadline	Solved
rop-basic	20	10-06-2017 00:00:00	10-20-2017 00:00:00	21
rop-64	20	10-06-2017 00:00:00	10-20-2017 00:00:00	21
pop	20	10-06-2017 00:00:00	10-20-2017 00:00:00	21
puzzle	20	10-06-2017 00:00:00	10-20-2017 00:00:00	21
upto-retaddr	20	10-06-2017 00:00:00	10-20-2017 00:00:00	21
find-gadget	20	10-06-2017 00:00:00	10-20-2017 00:00:00	20
sprintf	20	10-06-2017 00:00:00	10-20-2017 00:00:00	18
rop-sorting	20	10-06-2017 00:00:00	10-20-2017 00:00:00	20
inc1	20	10-06-2017 00:00:00	10-20-2017 00:00:00	18
fmtstr-relro	20	10-06-2017 00:00:00	10-20-2017 00:00:00	10

Best Write-ups for Lab06

- rop-basic: poning, carterchen
- rop-64: nagendra, carterchen
- pop: myao42, jallen309
- puzzle: nagendra, shudak3
- upto-retaddr: poning, dhaval
- find-gadget: N/A, N/A
- sprintf: markwis, jallen309
- rop-sorting: poning, brian_edmonds
- inc1: nagendra, carterchen
- fmtstr-relro: whuang328, jallen309

Discussion: Lab07

- What's the most "difficult" bug or challenge?
- What's the most "interesting" bug or challenge?
- So, ROP is too powerful?

Discussion: pop

- What was the challenging part?
- How did you solve?

Discussion: pop

Discussion: puzzle

- What was the problem?
- How did you solve?

Discussion: puzzle

- PALLET = "ALPHABETS : ABCDEFGHIJKLMNOPQRSTUVWXYZ_ "
- → "ROP_ATTACK_SUCCESS"

Discussion: upto-retaddr

- What was the problem?
- How did you solve?

Discussion: upto-retaddr

- Stack pivoting

Discussion: find-gadget

- What was the problem?
- How did you solve?

Discussion: find-gadget

Discussion: sprintf

- How much did you try?
- Where did you stuck?

Discussion: sprintf

Discussion: sprintf

Discussion: rop-sorting

- How much did you try?
- Where did you stuck?

Discussion: inc1

- How much did you try?
- Where did you stuck?

Discussion: inc1

Discussion: fmtstr-relro

- What's special about this problem?

Discussion: fmtstr-relro

- RELRO: not able to overwrite got, but
    - atexit(), seen in previous lab?
    - real world: a bit complex

Discussion: fmtstr-relro

Discussion: fmtstr-relro

- PTR_MANGLE(func)?

Take-outs from ROP

- DEP/ASLR are not perfect solutions (pretty good mitigation?)
  - DEP: ret-to-lib, ROP
  - ASLR: code leakage
- What about stack canary? (what if we placed it together?)
- Lots of known defenses (e.g., CFI)

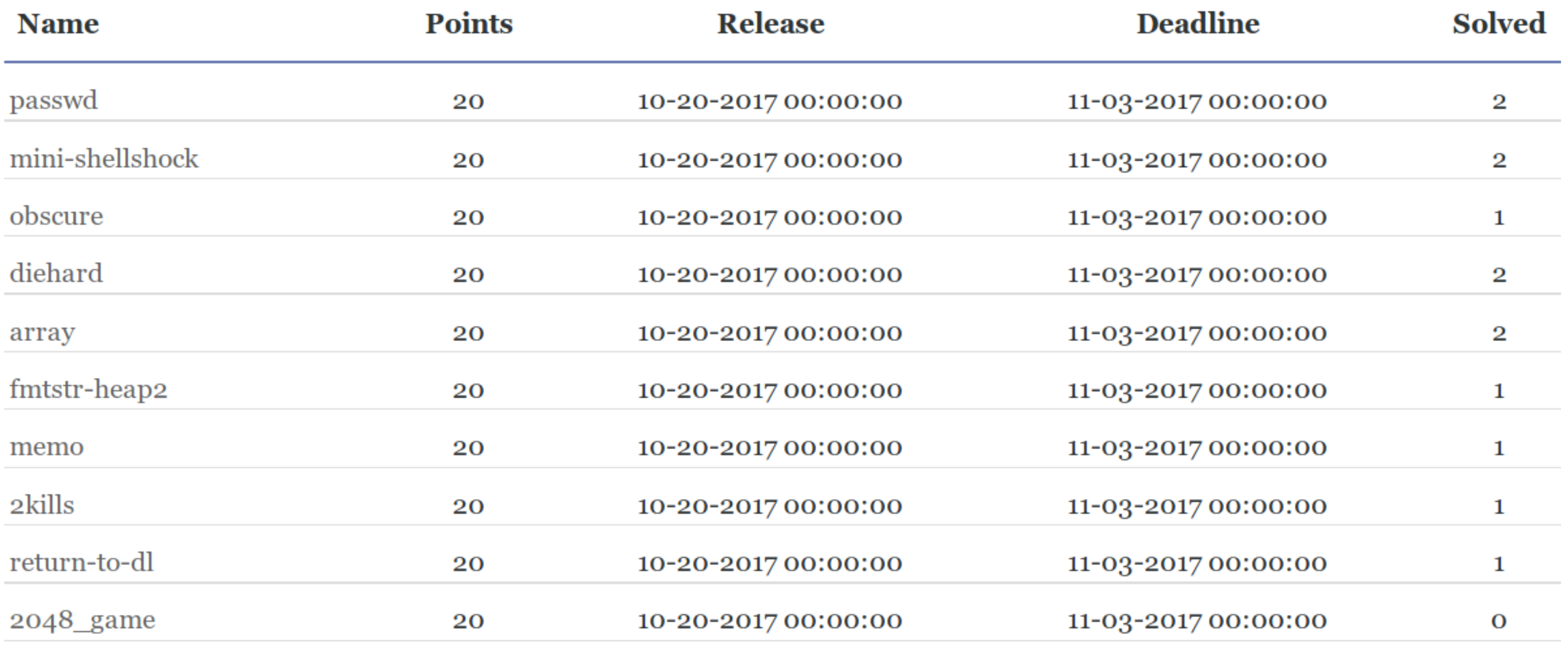
Today's Tutorial

- In-class tutorial:
  - Socket programming in Python
  - Your first remote exploit!

Remote Challenges

- Use techniques learned from Lab01-Lab07
- But targeting the remote server (e.g., online services)!

Lab08: Remote Challenges



Name	Points	Release	Deadline	Solved
passwd	20	10-20-2017 00:00:00	11-03-2017 00:00:00	2
mini-shellshock	20	10-20-2017 00:00:00	11-03-2017 00:00:00	2
obscure	20	10-20-2017 00:00:00	11-03-2017 00:00:00	1
diehard	20	10-20-2017 00:00:00	11-03-2017 00:00:00	2
array	20	10-20-2017 00:00:00	11-03-2017 00:00:00	2
fmtstr-heap2	20	10-20-2017 00:00:00	11-03-2017 00:00:00	1
memo	20	10-20-2017 00:00:00	11-03-2017 00:00:00	1
2kills	20	10-20-2017 00:00:00	11-03-2017 00:00:00	1
return-to-dl	20	10-20-2017 00:00:00	11-03-2017 00:00:00	1
2048_game	20	10-20-2017 00:00:00	11-03-2017 00:00:00	0

DEMO: about how remote challenges work

- nc
- exploit.py

In-class Tutorial

- Step1: nc
- Step2: brute force attack
- Step3: guessing attack

```
$ ssh YOURID@cyclonus.gtisc.gatech.edu -p 2023
$ ssh YOURID@cyclonus.gtisc.gatech.edu -p 2022
$ ssh YOURID@computron.gtisc.gatech.edu -p 2023
$ ssh YOURID@computron.gtisc.gatech.edu -p 2022

$ cd tut/lab08
$ cat README
```