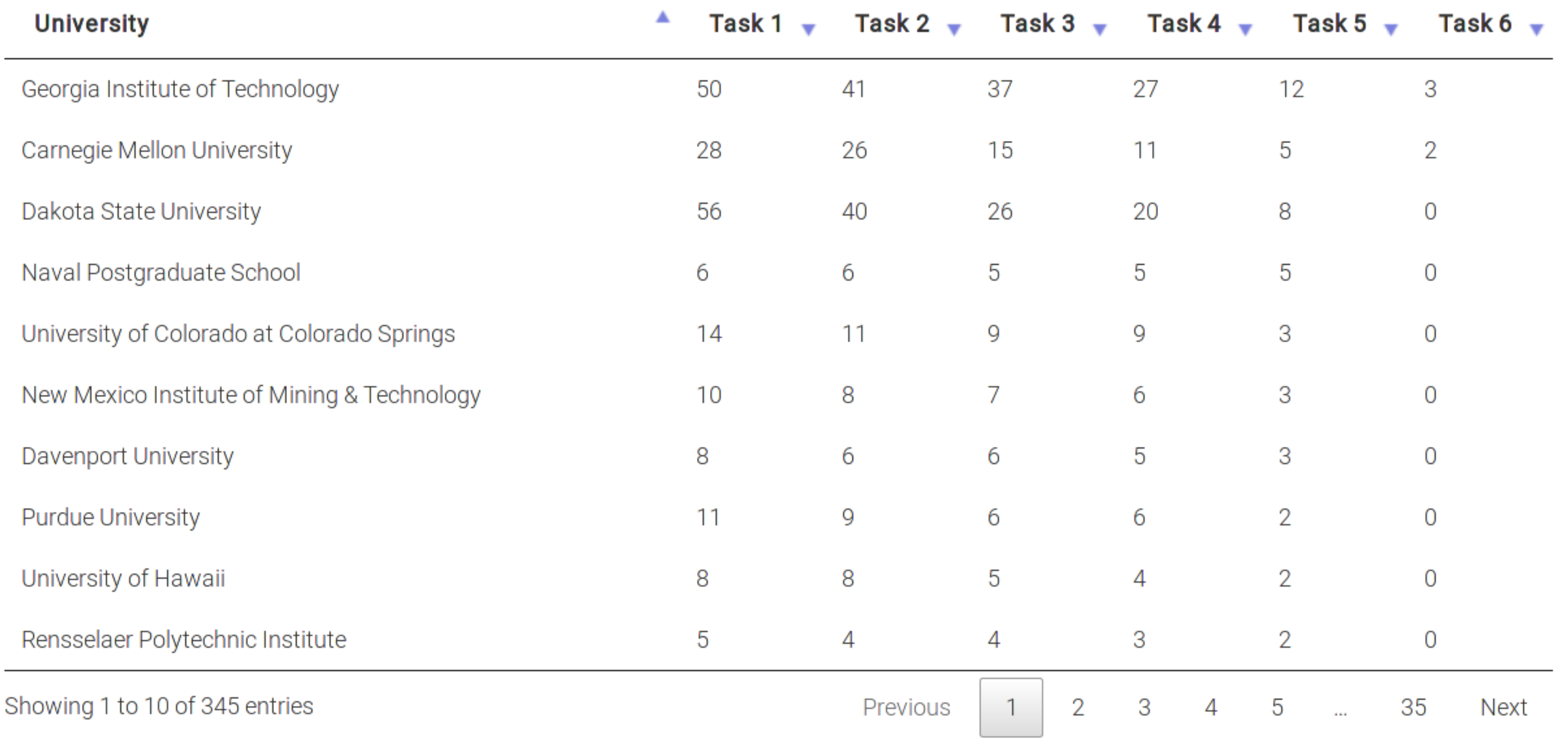
Lec08: Remote Exploit

Taesoo Kim

Scoreboard

NSA Codebreaker Challenges



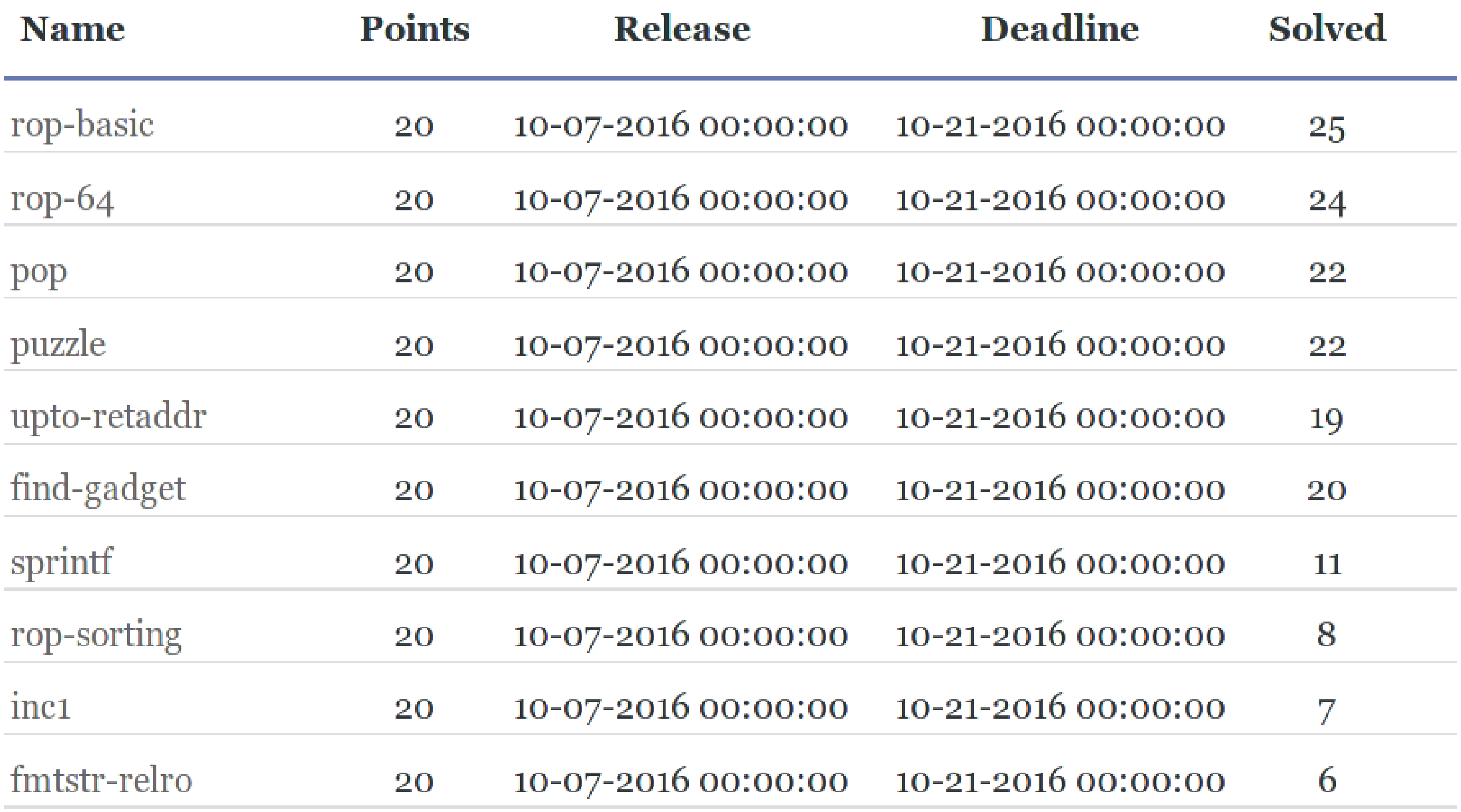
University	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6
Georgia Institute of Technology	50	41	37	27	12	3
Carnegie Mellon University	28	26	15	11	5	2
Dakota State University	56	40	26	20	8	0
Naval Postgraduate School	6	6	5	5	5	0
University of Colorado at Colorado Springs	14	11	9	9	3	0
New Mexico Institute of Mining & Technology	10	8	7	6	3	0
Davenport University	8	6	6	5	3	0
Purdue University	11	9	6	6	2	0
University of Hawaii	8	8	5	4	2	0
Rensselaer Polytechnic Institute	5	4	4	3	2	0

Showing 1 to 10 of 345 entries

Administrivia

- No class on Oct 28
- If you are interested in, check out EKOPARTY CTF 2016
- Due: Lab08 is out and its due on Nov 3 (two weeks!)
- NSA Codebreaker Challenge → Due: Dec 1

Lab06: ROP



Name	Points	Release	Deadline	Solved
rop-basic	20	10-07-2016 00:00:00	10-21-2016 00:00:00	25
rop-64	20	10-07-2016 00:00:00	10-21-2016 00:00:00	24
pop	20	10-07-2016 00:00:00	10-21-2016 00:00:00	22
puzzle	20	10-07-2016 00:00:00	10-21-2016 00:00:00	22
upto-retaddr	20	10-07-2016 00:00:00	10-21-2016 00:00:00	19
find-gadget	20	10-07-2016 00:00:00	10-21-2016 00:00:00	20
sprintf	20	10-07-2016 00:00:00	10-21-2016 00:00:00	11
rop-sorting	20	10-07-2016 00:00:00	10-21-2016 00:00:00	8
inc1	20	10-07-2016 00:00:00	10-21-2016 00:00:00	7
fmtstr-relro	20	10-07-2016 00:00:00	10-21-2016 00:00:00	6

Discussion: Lab07

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

Discussion: pop

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

Discussion: pop

Discussion: puzzle

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

Discussion: upto-retaddr

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

Discussion: find-gadget

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

Discussion: sprintf

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

Discussion: rop-sorting

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

Discussion: inc1

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

Discussion: fmtstr-relro

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

Take-outs from ROP

- DEP/ASLR are not perfect solutions
    - DEP: ret-to-lib, ROP
    - ASLR: code leakage
- What about stack canary? (what if we placed it together?)
- Lots of known defenses (did you attend today's talk?)

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)

DEMO: about how remote challenges work

- nc
- exploit.py

In-class Tutorial

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

```
$ git git@clone tc.gtisc.gatech.edu:seclab-pub cs6265
or
$ git pull
$ cd cs6265/lab08
$ ./init.sh

$ cd tut
$ cat README
```

Lec08: Remote Exploit

Taesoo Kim