

CS6265: Information Security Lab

Taesoo Kim

CS6265: Info. Security Lab

- A special course: supervised, **hands-on laboratory**
- Focusing on *reverse engineering* and *binary exploitation*
- Designed for seniors and above (including InfoSec MS, fresh PhDs)
 - Prerequisite: OS, system programming, architecture
 - Background: low-level programming (e.g., C, asm)

Goal: Think like an Attacker!



Learning via Capture-the-flag



CTF: Cyber War Game

- Jeopardy
- Attack and defense

Discover Our Unique Challenges Menu

Amuse Bouche	Signature Dishes
ELF Crumble warmup (Ordered by 368 teams) 102pt	www pwn (Ordered by 10 teams) 240pt
You Already Know warmup (Ordered by 487 teams) 101pt	adamtune misc, ml (Ordered by 3 teams) 416pt
Easy Pisy crypto, web (Ordered by 190 teams) 104pt	SAG? crypto, reverse (Ordered by 11 teams) 228pt
babypwn1805 pwn (Ordered by 39 teams) 132pt	stumbler reversing (Ordered by 11 teams) 228pt
sbva web (Ordered by 99 teams) 110pt	Ps-Secure reverse, x86-64 (Ordered by 7 teams) 291pt



Topics

- Reverse engineering
- Binary exploitation
- Bug finding
- Memory forensic
- etc.

Schedule: <https://tc.gts3.org/cs6265/2019/cal.html>

Big Picture: Course Structure

- Total 9 labs (week/bi-weekly)
- In-class CTF Nov 22 (i.e., 24h, Fri-Sat)
 - Prizes (\$1,000), 3 per team
 - Each team prepares one challenge for other teams

Weekly Structure

- **Fri** : Cover a single topic/theme (e.g., stack overflow)
- **Mon/Wed** : Optional recitations
 - 18:00-19:00 in **CoB 053** (Mon)
 - 18:00-19:00 in **CoB 052** (Wed)
- **Thr** : Deadline for the current week's problem set (i.e., 10 challenges)
 - Submit: **flag, write-up, and exploit** of **each** challenges

In-class Meeting (on Fri)

- 30 min: discuss last week's challenges (you will be asked to explain)
- 30 min: cover this week's topic
- 30-60 min: in-class tutorial (so bring your laptop!)
- 30-60 min: TA-ing

Course Grading

- *100% Lab* (no single lab returned → F)
 - **A**: 7+ challenges
 - **B**: 5+ challenges
 - On-site CTF: counted worth 2 labs
- No midterm/final exams
- Grading per group: undergrads, MSes and PhDs
- Check [Game Rules!](#)

Scoring Each Lab (Game Rules)

- For each of **10 challenges** (+ one in-class tutorial),
 - Submit a flag with corresponding write-up/exploit
 - Total **220pt**: $20\text{pt} \times 10 \text{ challenges} + 20\text{pt} \times 1 \text{ tutorial}$
- **Bonus**: two fastest solvers (aka, first/second bloods) $\rightarrow +2\text{pt}/+1\text{pt}$
- **Bonus**: best write-up/active participation $\rightarrow +1\text{pt}$
- **Late policy**: 50% of the original points (one extra week)

Online Competition

[Class](#) | [Problems](#) | [Scoreboard](#) | [Status](#) | [Chart](#)

[New api-key](#)

lab11

Name	Points	Release	Deadline	Solved	Flag	Exploits
sandbox-pttrace	20	11-18-2016 00:00:00	12-01-2016 00:00:00	9	Submit	Submit
sandbox-seccomp	20	11-18-2016 00:00:00	12-01-2016 00:00:00	4	Submit	Submit
sandbox-pttrace2	20	11-18-2016 00:00:00	12-01-2016 00:00:00	8	Submit	Submit
srop	20	11-18-2016 00:00:00	12-01-2016 00:00:00	7	Submit	Submit
simple-aeg	20	11-18-2016 00:00:00	12-01-2016 00:00:00	3	Submit	Submit
sandbox-pin	20	11-18-2016 00:00:00	12-01-2016 00:00:00	1	Submit	Submit
kproc-zeropage	20	11-18-2016 00:00:00	12-01-2016 00:00:00	2	Submit	Submit
kproc-bufovfl	20	11-18-2016 00:00:00	12-01-2016 00:00:00	1	Submit	Submit
kproc-ret2dir	20	11-18-2016 00:00:00	12-01-2016 00:00:00	0	Submit	Submit
kproc-uaf	20	11-18-2016 00:00:00	12-01-2016 00:00:00	0	Submit	Submit

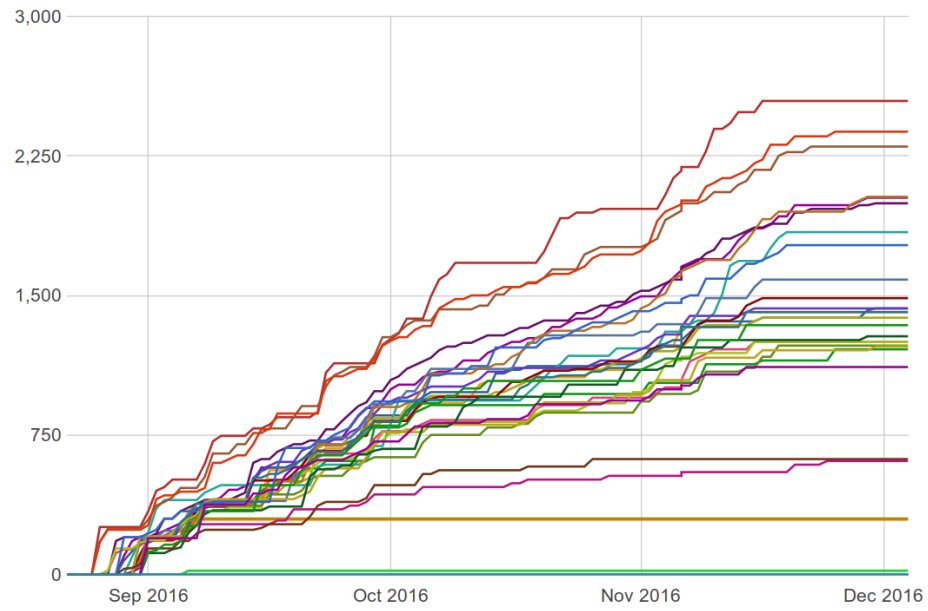
lab10

Name	Points	Release	Deadline	Solved	Flag	Exploits
dlmalloc	20	11-11-2016 00:00:00	12-01-2016 00:00:00	20	Submit	Submit
ptmalloc	20	11-11-2016 00:00:00	12-01-2016 00:00:00	14	Submit	Submit
uaf-basic	20	11-11-2016 00:00:00	12-01-2016 00:00:00	23	Submit	Submit
heap-spray	20	11-11-2016 00:00:00	12-01-2016 00:00:00	20	Submit	Submit

Online Competition

[Class](#) | [Problems](#) | [Scoreboard](#) | [Status](#) | [Chart](#)

Score Charts



Tips for CS6265

- Study in group (e.g., discussion)
- Come to the recitation!
- Understand your time budget
- Tackle challenges in order
- Learn basic tools next two weeks (e.g., editor, debugger, python)

Misconduct Policy

- Cheating vs. collaboration
- Refer [GT's Academic Misconduct Policy](#)
- ***Never ever*** use/copy other students' code/write-up
- Please ***write down names*** of your collaborators

About Course Material

- You should ***never*** share exploits/write-up online
- Once found → F (even after the semester is over)
- We are checking your submission against past years' submissions

Administrivia



- TA: Fan Sang, Seulbae Kim, Ren Ding, Jung-Won Lim, Yongwhi Jin
- Contact: 6265-staff@cc.gatech.edu
- Website: <https://tc.gts3.org/cs6265/2019/>
- Piazza: <https://piazza.com/gatech/fall2019/cs6265/home>

TA Rules

- Please come to the recitation
 - 6-7pm in CoB 053/054 on Mon/Wed
- Please post your questions on [Piazza](#)
 - Proactively participate the online discussion!
- Contact 6265-staff@cc.gatech.edu to make an appointment

Next Two Weeks

Monday	Tuesday	Wednesday	Thursday	Friday
Aug 19 First day of class (No class)	Aug 20	Aug 21	Aug 22	Aug 23 LEC 1: Warm-up: x86, Tools Preparation: Read asm Assigned: Lab 01: Bomb Lab1
Aug 26	Aug 27	Aug 28 REC 1: Lab 01	Aug 29 DUE: Lab 01	Aug 30 LEC 2: Warm-up: x86_64, Shellcode, Tools TUT 1: pwndbg, Shellcode (link) Preparation: Read x86_64 Assigned: Lab 02: Bomb Lab2 / Shellcode
Sep 2 Labor day	Sep 3	Sep 4 REC 2: Lab 02	Sep 5 DUE: Lab 02	Sep 6 LEC 3: Writing exploits TUT 2: Writing Your First Exploit Preparation: Read Phrack #49-14 Assigned: Lab 03: Stack Overflow

Today's Topics

- This week: **Bomblab** !
- Quick introduction to GDB
- In-class tutorial
 - Walk over x86 asm and tools
 - Be familiarized with GDB and x86 (32-bit)
 - Let's crack crackme0x00–crackme0x04 binaries

Note on Flag

- Random looking bytes, but be careful. It is designed to include tons of information unique to you, so we can easily check plagiarism

```
$ cat /proc/flag
```

```
CB25682B33EF8BF23545A767562A1D5AA33C88EEACC1AE562D950CB9F1E5725D  
864725DB51460902ECBD52BA4CBED86A10F3A98A35F6FB71871019702A0E9199  
5BC59332C390A3C27D0EC2CE85BC13E956A6027E3171352F90467A8C12346D9A  
2A26EE914B3078ED031FDB14BB6224C3D743D79A733FB49EB4E9C1F383CF810E  
F6841EE935FE2DA2C57DB4804B6823884B36AE62B08848486918C120E4C2AA94  
E1D3F8A6E9E2251AC39E5F37971FB07DFF839E0BC1C4E6C1D4A24E0948F8751B  
25BFFE854CD84A8D8E28814398FF192CD9AD37150D83DA872E944DF1552F97DD
```

```
...
```

Note on Bomblab

```
$ ./bomb
```

```
Enter your api-key: <paste-your-api-key>
```

```
      ,---.!,  
    __/  -*  |_____)  _____| |____| |____| |____| |____| |____|  
,d08b.  '|`  | _ \ / _ \ | ' _ ` _ \ | ' _ \ | / _ ` | ' _ \  
0088MM   | |_) | ( _ ) | | | | | | | | | |_) | | ( _ | |_) |  
`9MMP'   |____/ \____/ | | | | | | | | | |____/ | | \____, _ | |____/ |  
        cs6265
```

```
Welcome to my fiendish little bomb. You have N? phases with  
which to blow yourself up. See you alive!
```

```
(hint: security question)
```

```
>
```

Note on Explosion

```

      __,--~/~      `-----
     _/_,----(      ,      )
    _/_/      <      /      ) \___
-----===; ; ; '====-----===; ; ;====-----
  \/_  ~'~'~'~'~'~'\~'~)~'/_
  (_ ( \ ( > \)
  \_( _ < >_>'
    ~ ` -i' ::>|--'
      I;|.|. |
    <|i::|i|\` .
    (` ^''`-' ' )

```

DEMO: GDB Summary

- run/continue
- break/tbreak/rbreak/delete
- stepi/nexti/advance/finish
- info reg/proc/break
- backtrace/examine
- python, gdbinit
- etc.

In-class Tutorial

- Step 1: Setup the game environment
 - <https://tc.gts3.org/cs6265/2019/rules.html>
- Step 2: Tutorial (in CTF servers)
 - <https://tc.gts3.org/cs6265/2019/tut/tut01-warmup.html>

```
$ ssh lab01@3.223.237.92
```

```
password:
```

```
$ cat README
```

```
$ cd tut01-crackme
```

```
$ cat README
```

References

- [GDB tutorial](#)
- [x86 instructions](#)
- [x86 architecture](#)