CS6265: Information Security Lab

Taesoo Kim

CS6265: Information Security Lab

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

Course Goal: Think like an Attacker!

Learning by Playing Capture-the-flag (CTF)

CTF: a Cyber War Game

- Jeopardy
- Attack and defense

Topics

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

Schedule: https://tc.gts3.org/cs6265/2018/cal.html

Big Picture: Course Structure

- Total 9–10 labs (week/bi-weekly)
- New this year: In-class CTF Nov 16–17
  - By team
  - Prizes
  - Each team prepares one challenge for other teams

Weekly Structure

- Fri: Cover a single topic/theme (e.g., stack overflow)
- Wed : Recitation from 5 to 6pm in Klaus 1447 (optional)
- Thr : Deadline for the current week's problem set (i.e., 10 challenges)
  - Submit: flag, write-up, and exploit of each challenge

In-class Meeting (on Fri)

- 30 min: discus 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 (if you didn't turn in a single lab, you will get F)
- No midterm and final exams
- 40%: A, 30-40%: B, 30-20%: C and below
  - If you solve 7 challenges on average, you will get A
- Grading in each group: undergrads, MSes and PhDs
- Check Game Rules!

Scoring Each Lab (Game Rules)

- For each of **10 challenges** (+ one in-class tutorial),
  - Get a flag and submit it with corresponding write-up/exploit
  - Total 220pt : 20pt x 10 challenges + 20pt x 1 tutorial
  - Hint : Losing 5–10pt
- Bonus : two fastest solvers (aka, first/second bloods) get 10pt and 5pt
- Late policy : 50% of the original points (an extra week)

Online Competition

Class | Problems | Scoreboard | Status | Chart New api-key

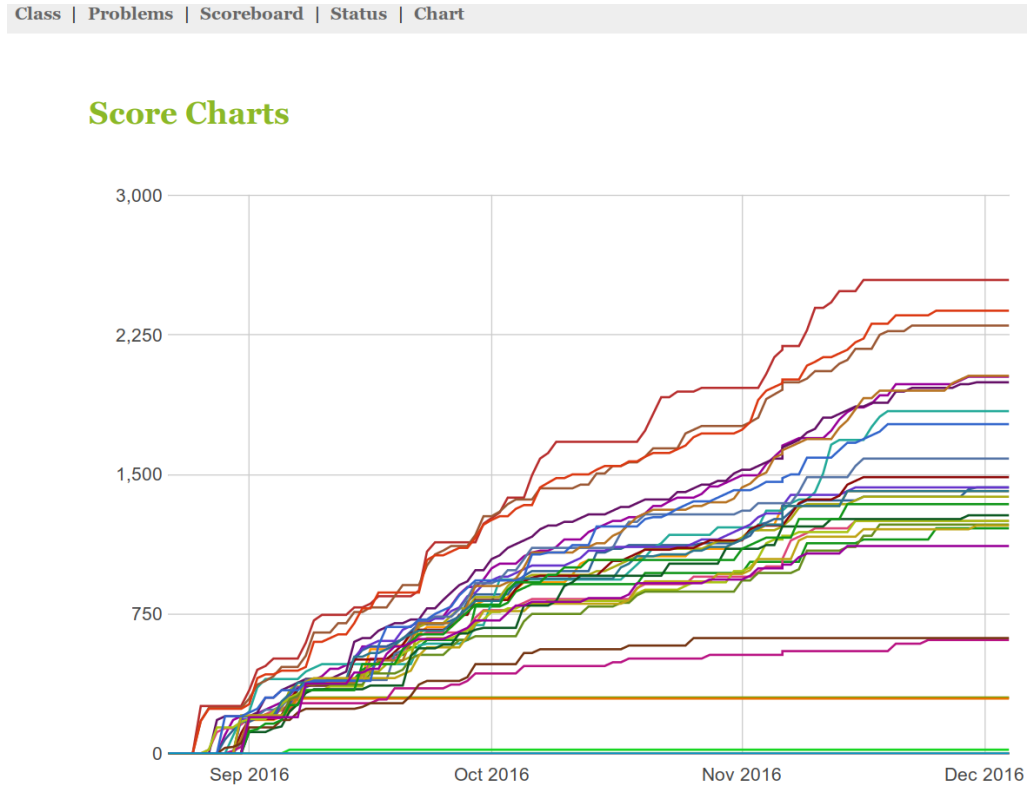
lab11

Name	Points	Release	Deadline	Solved	Flag	Exploits
sandbox-ptrace	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-ptrace2	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



Tips to Complete CS6265 Successfully

- Study in group (e.g., discussion)
- Come to the recitation
- Understand your time budget
- Tackle binaries 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, you will get F (even after the semester)
- We are checking your submission with past years' submissions

Administrivia

- TA: Insu Yun, Soyeon Park, Dhaval Kapil (online) + N volunteers!
- Contact: 6265-staff@cc.gatech.edu
- Website: https://tc.gts3.org/cs6265/2018/
- Piazza: https://piazza.com/gatech/fall2018/cs6265/home

TA Rules

- Please come to the recitation: 5-6pm in Klaus 1447 on Wed
- Please post your questions on Piazza
- Contact 6265-staff@cc.gatech.edu to make an appointment

Next Two Weeks

Monday	Tuesday	Wednesday	Thursday	Friday
Aug 20 *First day of class (**No class**)*	Aug 21	Aug 22	Aug 23	Aug 24 **LEC 1:** Warm-up: x86, Tools **TUT 1:** GDB/x86 **Preparation:** Read asm **Assigned:** Lab 01: Bomb Lab1
Aug 27	Aug 28	Aug 29 **REC 1:** Lab 01	Aug 30 **DUE:** Lab 01	Aug 31 **LEC 2:** Warm-up: x86_64, Shellcode, Tools **TUT 2:** PEDA, Shellcode (video/slides) **Preparation:** Read x86_64 **Assigned:** Lab 02: Bomb Lab2 / Shellcode
Sep 3 Labor day	Sep 4	Sep 5 **REC 2:** Lab 02	Sep 6 **DUE:** Lab 02	Sep 7 **LEC 3:** Writing exploits **TUT 3:** IDA, Your first control hijacking **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
...
```

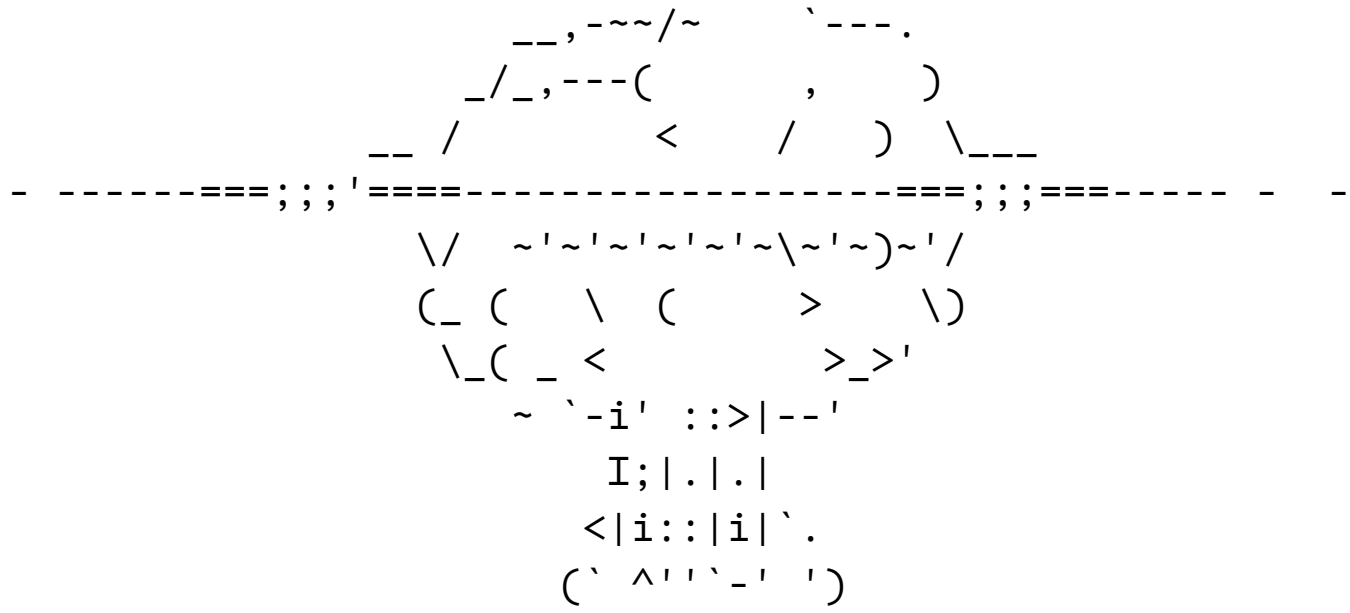
Note on Bomblab

```
$ ssh lab01@computron.gtisc.gatech.edu -p 9001
$ ./bomb [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



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/cs6265/2018/rules.html
- Step 2: Tutorial (in CTF servers)

```
$ ssh lab01@cyclonus.gtisc.gatech.edu -p 9001
or
$ ssh lab01@computron.gtisc.gatech.edu -p 9001
Password: lab01

$ cat README
$ cd tut01-crackme
$ cat README
```

References

- GDB tutorial
- x86 instructions
- x86 architecture