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 MS, 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

Topics

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

Schedule: https://tc.gts3.org/cs6265/2020-winter/

Topics

Week1. Lab: Bomb Lab1
Week2. Lab: Bomb Lab2 / Shellcode
Week3. Lab: Stack Overflow
Week4. Lab: Bypassing Stack Protection
Week5. Lab: Bypassing DEP/ASLR
Week6. Lab: Return-oriented Programming
Week7. Lab: Remote Attacks
Week8. Lab: Miscellaneous Topics

Big Picture: Course Structure

- Total 8 labs, one lab per week!
- One optional bonus lab about heap exploitation

Monday	Tuesday	Wednesday	Thursday	Friday
Dec 21 **LEC:** Warm-up: x86, Tools (slides, slides) **TUT:** Tut01: GDB/x86 **Preperation:** Read asm **Assigned:** Lab01: Bomb Lab1	Dec 22	Dec 23	Dec 24 **REC:** Lab 01	Dec 25 Christmas
Dec 28 **LEC:** Warm-up: x86_64, Shellcode, Tools (slides, slides) **TUT:** Tut02: Pwndbg, Ghidra, Shellcode [video1],[video2],[video3] **Preperation:** Read x86_64 **Assigned:** Lab02: Bomb Lab2 / Shellcode **DUE:** Lab 01	Dec 29	Dec 30	Dec 31 **REC:** Lab 02	Jan 01 New Year's

Weekly Structure

- Mon 09:00-10:30 : in-class meeting/review (watch lecture/tutorial video ahead)
- Mon 10:30-12:00 : in-class tutorial/recitation (optional)
- Thu 09:00-12:00 : individual help/tutoring on challenges (optional, office hours)
- Fri : Release the new lab (**9am**)!
- Mon : Deadline for the current week's problem set (**9am**)!
  - Submit: flag, write-up, and exploit of each challenges

General Rule

- 1-2 tutorials and 10 challenges every week will be announced
- 20 points (flag) x 1.0 (write-up/exploit) = 20 points (each challenge)
- 220 points (20 points x 11 challenges) are the maximum points, in theory
- Bonus : first two fastest solvers get 2/1 bonus pt for each challenge
- Hint : We will provide up to two hints on each challenge (in the submission site)
- Late policy : 50% of the original points (for two weeks past the due date)

Grading

- All tutorials (1-2 per week) plus 4-5 challenges per lab → A
  - Lab 1-2: 5, Lab 3-8: 4 → 11 tutorials + 34 challenges, 900 pt
  - B/C/D will be determined later (hope all get A)!
  - **No tutorial** submitted → F

Tips for CS6265

- Study in group (e.g., discussion) → Join Mattermost and Piazza.
- Come to the recitation → Thursday 09:00-12:00!
- Understand your time budget
- Tackle challenges in order
- Learn basic tools next two weeks (e.g., editor, debugger, python)

Note on Submission Site

Note on Submission Site

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
...
```

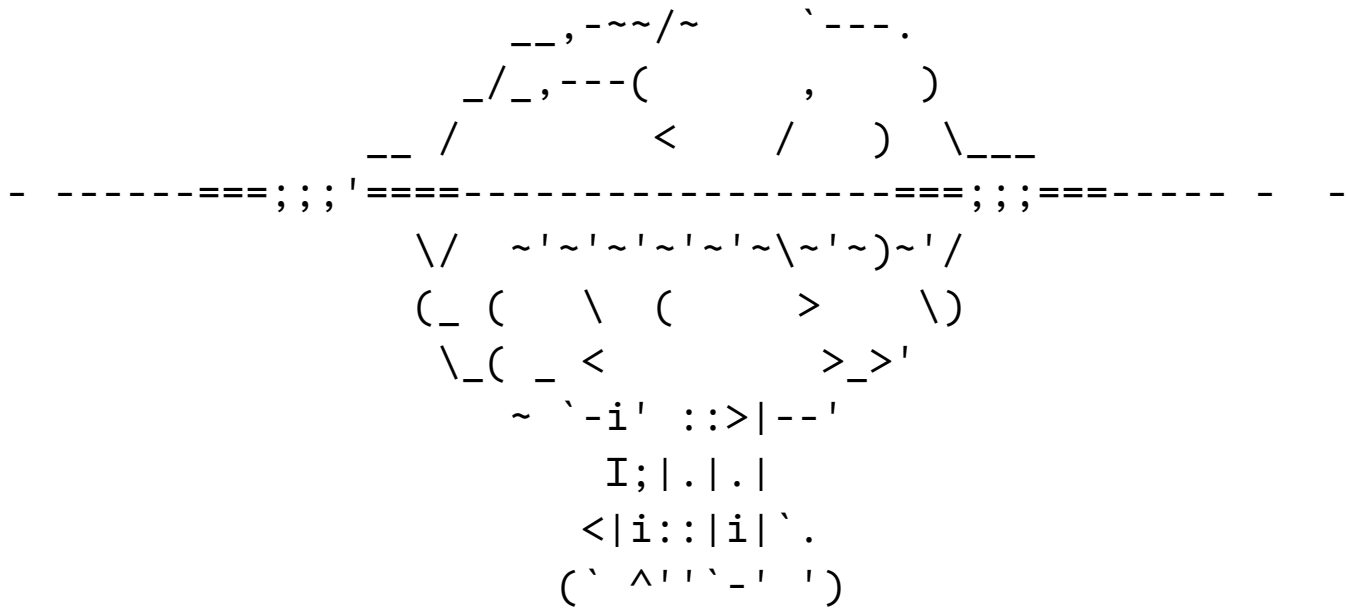
Note on Bomblab


```
$ ./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



DEMO: GDB Summary

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

Summary

1. Class website
2. Piazza
3. Mattermost
4. Submission site

All announces will be made both eTL and Piazza!

In-class Tutorial

- Step 1: Setup the game environment
  - https://tc.gts3.org/cs6265/2020-winter/rules.html
- Step 2: Tutorial (in CTF servers)
  - https://tc.gts3.org/cs6265/2020-winter/tut/tut01-warmup.html

```
$ ssh lab01@ss.snucse.org
password:

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

References

- GDB tutorial
- x86 instructions
- x86 architecture