Lec09: Miscellaneous

Max Wolotsky

Happy Halloween :)

Scoreboard

NSA Codebreaker Challenges

Solution Totals

Show 10 entries

Search:

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	32	19	16	8	5	3	0
University of Hawaii	21	10	8	4	3	2	0
Pennsylvania State University	53	14	11	6	3	1	0
University of Tulsa	14	6	6	5	2	1	0
Virginia Community College System	14	2	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	28	13	11	3	1	0	0

Showing 1 to 10 of 421 entries

Previous 1 2 3 4 5 ... 43 Next

Administrivia

- Due: Lab09 is out and its due on Nov 10
- NSA Codebreaker Challenge → Due: Dec 1

Discussion: Lab08

lab08

Name	Points	Release	Deadline	Solved
passwd	20	10-20-2017 00:00:00	11-03-2017 00:00:00	21
mini-shellshock	20	10-20-2017 00:00:00	11-03-2017 00:00:00	22
obscure	20	10-20-2017 00:00:00	11-03-2017 00:00:00	20
diehard	20	10-20-2017 00:00:00	11-03-2017 00:00:00	18
array	20	10-20-2017 00:00:00	11-03-2017 00:00:00	19
fmtstr-heap2	20	10-20-2017 00:00:00	11-03-2017 00:00:00	19
memo	20	10-20-2017 00:00:00	11-03-2017 00:00:00	8
2kills	20	10-20-2017 00:00:00	11-03-2017 00:00:00	20
return-to-dl	20	10-20-2017 00:00:00	11-03-2017 00:00:00	8
2048_game	20	10-20-2017 00:00:00	11-03-2017 00:00:00	12

Best Write-ups for Lab08

- passwd: shudak3, brian_edmonds
- mini-shellshock: shudak3, carterchen
- obscure: brian_edmonds, myao42
- diehard: mansourah, whuang328
- array: jallen309, brian_edmonds
- fmtstr-heap2: jallen309, brian_edmonds
- memo: carterchen, jallen309
- 2kills: luoyinfeng, N/A
- return-to-dl: whuang328, carterchen/markwis
- 2048_game: shudak3, jallen309

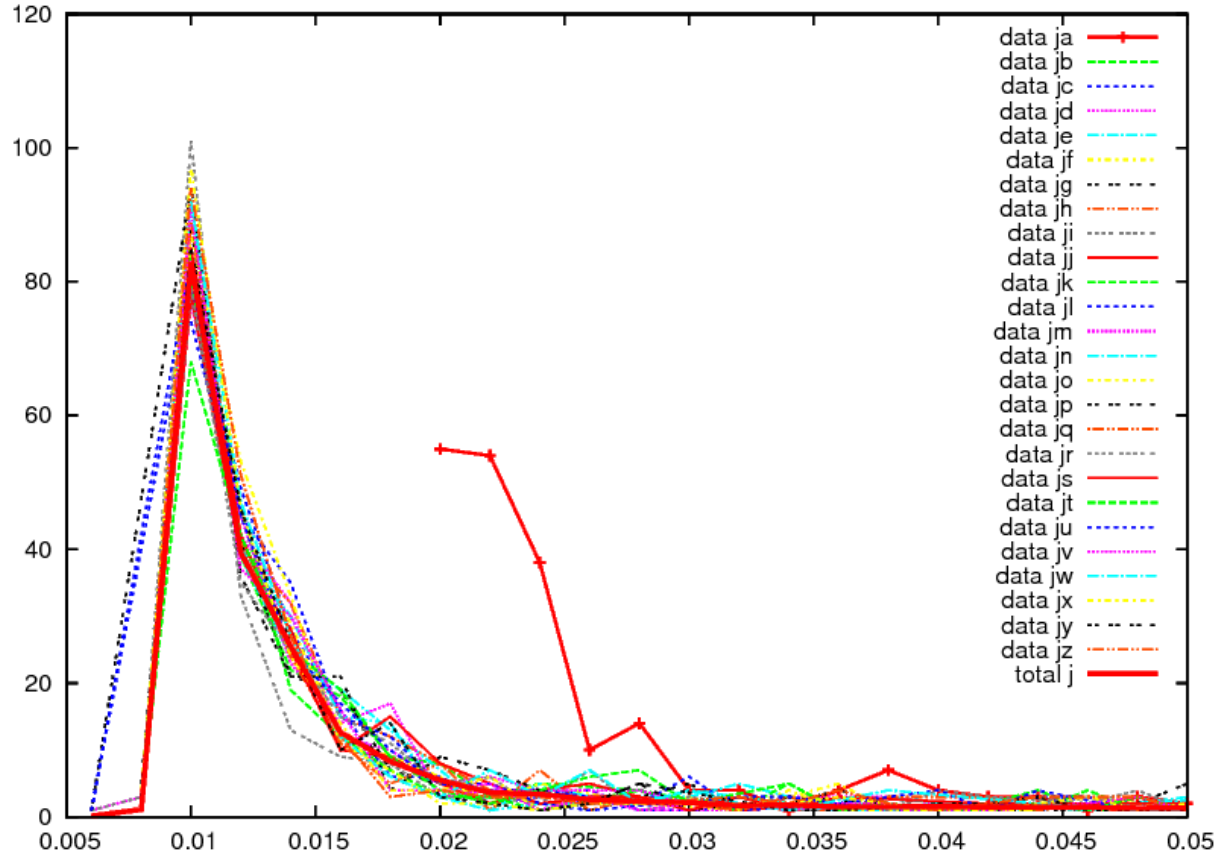
Discussion: Lab08

- What's the most "annoying" bug or challenge?
- What's the most "interesting" bug or challenge?
- What's different between remote & local?

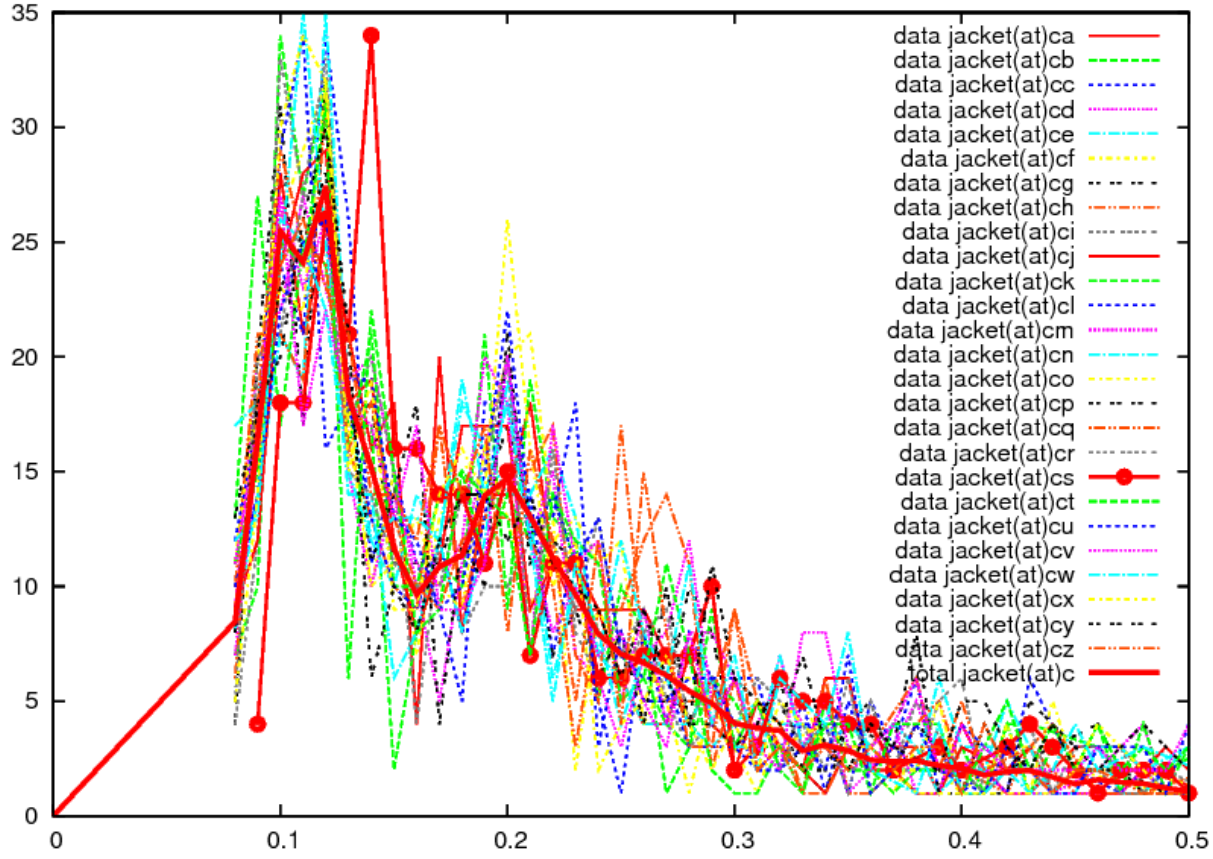
Discussion: passwd

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

Discussion: passwd



Discussion: passwd



Discussion: mini-shellshock

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

Discussion: mini-shellshock

- CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186
- Specially crafted environment variable

Discussion: mini-shellshock

- CGI (Common Gateway Interface)
  - HTTP headers → Environment variable
  - If script is a *bash* script?

Discussion: mini-shellshock

Discussion: obscure

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

Discussion: obscure

- ARM
  - different calling convention
  - r0: first argument

Discussion: obscure

```
__libc_csu_init (int argc, char **argv, char **envp)
 {
   const size_t size = __init_array_end - __init_array_start;
   for (size_t i = 0; i < size; i++)
       (*__init_array_start [i]) (argc, argv, envp);
}
```

Discussion: obscure

```
.text:00008610          ADD     R4, R4, #1
.text:00008614          LDR     R3, [R5,#4]!
.text:00008618          MOV     R0, R7          // R0 = R7
.text:0000861C          MOV     R1, R8
.text:00008620          MOV     R2, R9
.text:00008624          BLX     R3              // EIP = R3
.text:00008628          CMP     R4, R6
.text:0000862C          BNE     loc_8610
.text:00008630          LDMFD   SP!, {R3-R9,PC} // R3...R9 & PC
```

Discussion: diehard

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

Discussion: array

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

Discussion: fmtstr-heap2

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

Discussion: memo

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

Discussion: 2kills

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

Discussion: return-to-dl

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

Discussion: return-to-dl

- How GOT works?
- make fake SYMTAB, STRTAB ...

Discussion: 2048_game

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

Discussion: 2048_game

- How to calculate address?

Discussion: 2048_game

- Using format string, arbitrary read!
- Extract binary is also possible

Lab09: Miscellaneous

- integer overflow
- web
- race condition
- interesting exploit techniques

Today's Tutorial

- In-class tutorial:
  - Writing reliable exploit
  - Logical vulnerability

Today's Tutorial

```
int main() {
    char buf[0x100];
    printf("Give me something...");
    fgets(buf, 2 * sizeof(buf), stdin);
}
```

Today's Tutorial

- [...][printf plt][pop ret][__libc_start_main GOT][main]

Today's Tutorial

- calculate system based on leaked address
- [...][system][XXXX][/bin/sh addr]

In-class Tutorial

```
$ ssh your_id@computron.gtisc.gatech.edu -p 2022~2024
or
$ ssh your_id@cyclonus.gtisc.gatech.edu -p 2022~2024

$ cd tut/lab09
$ cat README
```