Lec03: Writing Exploits

Taesoo Kim

Scoreboard

Administrivia

- Survey: how many hours did you spend? (<3h, 6h, 10h, 15h, >20h)
- Please join Piazza
- An optional recitation at 5-7pm on every Wed (in **CoC 052**)
- Lab02: deadline is extended for another week!
- Lab03: stack overflow callenges are out!
- Due : Sept 20th at midnight (2 weeks)

Survival Guide for CS6265

1. Work as a group/team (find the best ones around you!)
    - NOT each member tackles different problems
    - All members tackle the same problem (and discuss/help)
2. Ask questions wisely, concretely
    - Explain your assumption first (e.g., I expect A because …)
    - Explain your problem second (e.g., A is expected but B appears)
3. Take advantage of four TAs standing next you to help!
    - World-class hackers give a private tutoring for you!
    - But, remember! only when you ask ..

Thinking of Threat Model

- Story: A group of students modified “bomb” and got “flags”?
- Why TAs think they are not correct flags?
- How does our system validate flags?

Thinking of Threat Model

```
# Q0. can we get a flag like this?
$ cat /proc/flag
# Q1. how is this flag different from what bomb prints out?
$ echo "phase2" > /proc/flag# cat /proc/flag
# Q2. what about under a tracer?
$ strace -- cat /proc/flag
# Q3. what about this and print flag?
$ gdb ./bomb
# Q4. are they different? why?
$ diff <(cat /proc/flag) <(cat /proc/flag)
# Q5. what about this?
$ diff <(cat /proc/flag) <(sleep 1; cat /proc/flag)
```

Lab03: Stack overflow (due in two weeks)

- Finally! It's time to write real exploits (i.e., control hijacking)
- TONS of interesting challenges!
  - e.g., lack-of-four, frobnicated, upside-down ..

Today's Tutorial

- Example: hijacking crackme0x00!
- A template exploit code
- In-class tutorial
  - Your first stack overflow!
  - Extending the exploit template (python)

DEMO: IDA/crackme0x00

- IDA w/ crackme0x00
- Exploit writing

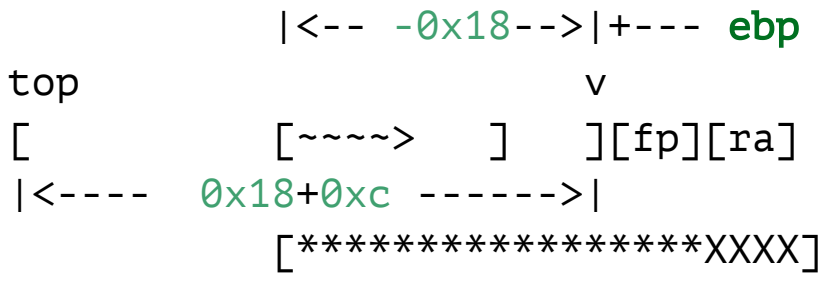
crackme0x00

```
$ objdump -M intel-mnemonic -d crackme0x00
...
0804869d <start>:
804869d: 55                             push   ebp
804869e: 89 e5                          mov    ebp,esp
80486a0: 83 ec 18                       sub    esp,0x18
80486a3: 83 ec 0c                       sub    esp,0xc
...
```

```
           |<-- -0x18-->|+--- ebp
top                     v
[          [buf ..  ]   ][fp][ra]
|<----  0x18+0xc ------>|
```

crackme0x00

```
$ objdump -M intel-mnemonic -d crackme0x00
...
80486c6: 8d 45 e8                lea    eax,[ebp-0x18]
80486c9: 50                       push   eax
80486ca: 68 31 88 04 08           push   0x8048831
80486cf: e8 ac fd ff ff           call   8048480 <scanf@plt>
```



crackme0x00

- How can we bypass the password check w/o putting the correct password?

In-class Tutorial

- Step 1: Navigate the binary with your IDA!
- Step 2: Play with your first exploit!
- Step 3: Using an exploit template!

```
$ ssh lab03@cyclonus.gtisc.gatech.edu -p 9003
$ ssh lab03@computron.gtisc.gatech.edu -p 9003
Password: lab03

$ cd tut03-stackovfl
$ cat README
```

References

- IDA Demo
- Phrack #49-14