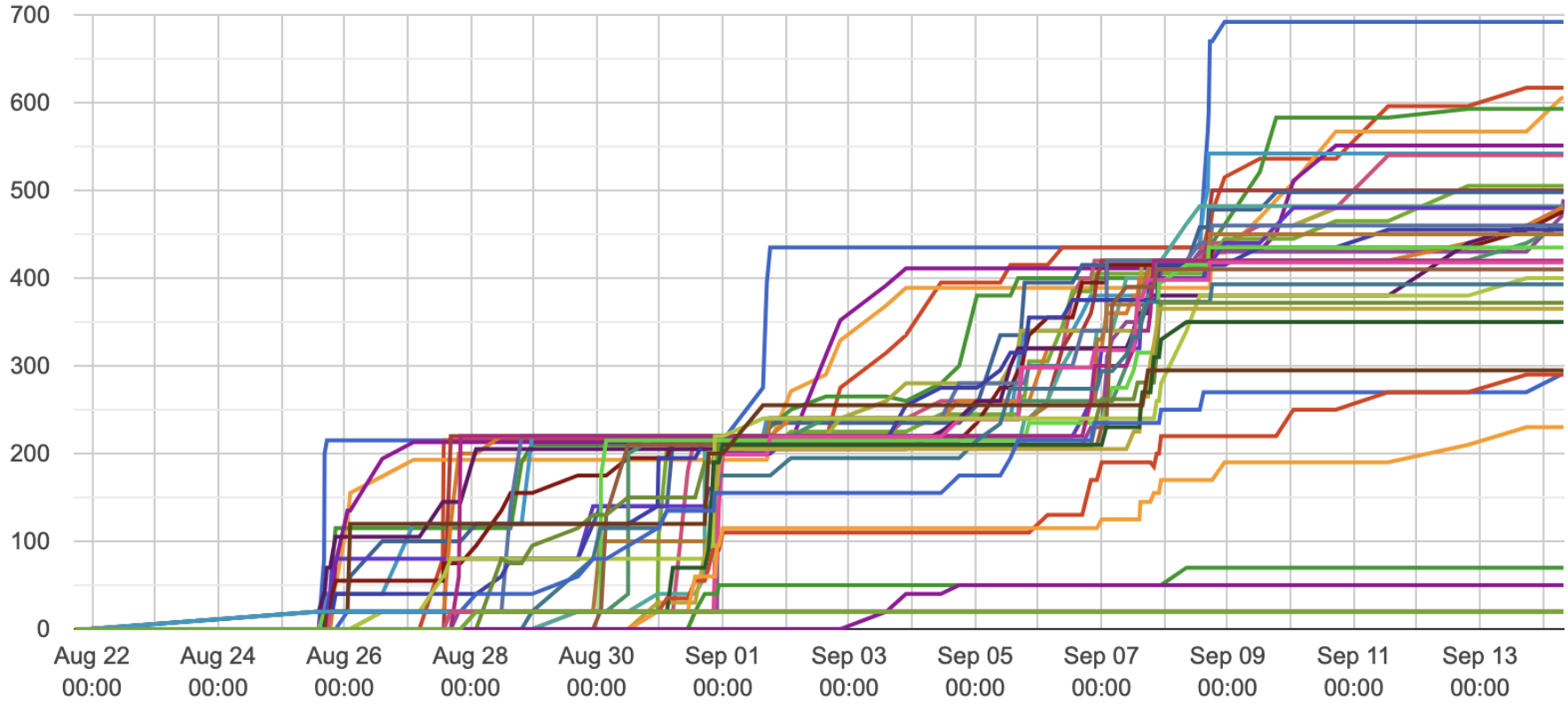
Lec04: Writing Exploits with Pwntools

Taesoo Kim

Scoreboad


700
600
500
400
300
200
100
0
Aug 22 00:00
Aug 24 00:00
Aug 26 00:00
Aug 28 00:00
Aug 30 00:00
Sep 01 00:00
Sep 03 00:00
Sep 05 00:00
Sep 07 00:00
Sep 09 00:00
Sep 11 00:00
Sep 13 00:00

Administrivia

- Please join Ed
- Optional recitations: Tue/Wed (@Coda)
- Due: Sep 21 at midnight (in a week)

Lab03: Stack overflow!

- 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: exploit crackme0x00 to get a shell/flag!
- Explore a template exploit code (PwnTool)
- In-class tutorial
  - Learning PwnTool
  - Writing your first stack overflow exploit!

Understanding Environment


```
$ cat /proc/self/maps | grep stack
7ffffffde000-7ffffffff000 rw-p 00000000 00:00 0  [stack]

$ cat /proc/self/maps | grep stack
7ffffffde000-7ffffffff000 rw-p 00000000 00:00 0  [stack]
```

Understanding Environment


```
$ checksec crackme0x00
[*] '/home/lab03/tut03-pwntool/crackme0x00'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x8048000)
    RWX:      Has RWX segments
```

Reminder: crackme0x00


```
$ objdump-intel -d crackme0x00
...
8048414:       push   ebp
8048415:       mov    ebp,esp
8048417:       sub    esp,0x28

                          +--- ebp
top                       v
[                        ][fp][ra]
|<=--   0x28  ------=>|
```

Reminder: crackme0x00

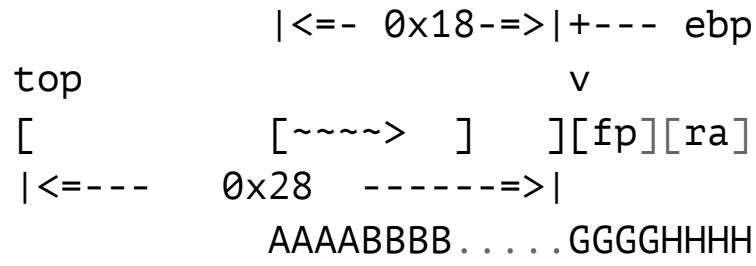

```
$ objdump-intel -d crackme0x00
...
8048448:       lea    eax,[ebp-0x18]
804844b:       mov    DWORD PTR [esp+0x4],eax
804844f:       mov    DWORD PTR [esp],0x804858c
8048456:       call   8048330 <scanf@plt>

            |<=- 0x18-=>|+--- ebp
top                      v
[           [~~~~>  ]    ][fp][ra]
|<=---    0x28  ------=>|
```

Reminder: crackme0x00


```
main() {
  char s1[16];
  ...
  scanf("%s", &s1);
  ...
}
```

Reminder: crackme0x00

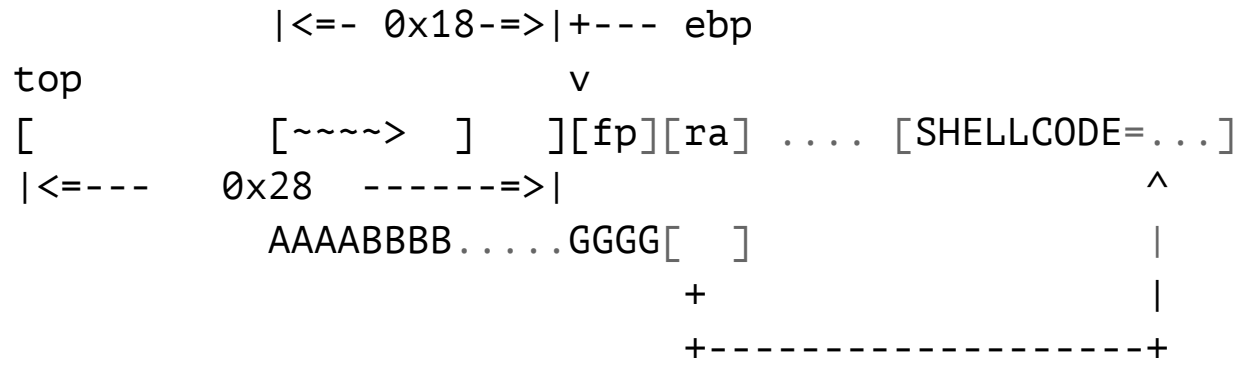


Where to put Shellcode?

- stack (today's tutorial)
- commandline argument
- environment vars
- ??

Injecting Shellcode (env)

1. How to decide the address of an environment variable? (changing?)
2. How to inject (or manipulate) environment variables?



In-class Tutorial

- Step 1: Learn PwnTool
- Step 2: Play with your first exploit!

```
$ ssh lab03@54.88.195.85
Password: xxxxxxxx

$ cd tut03-pwntool
$ cat README
```

References

- Phrack #49-14