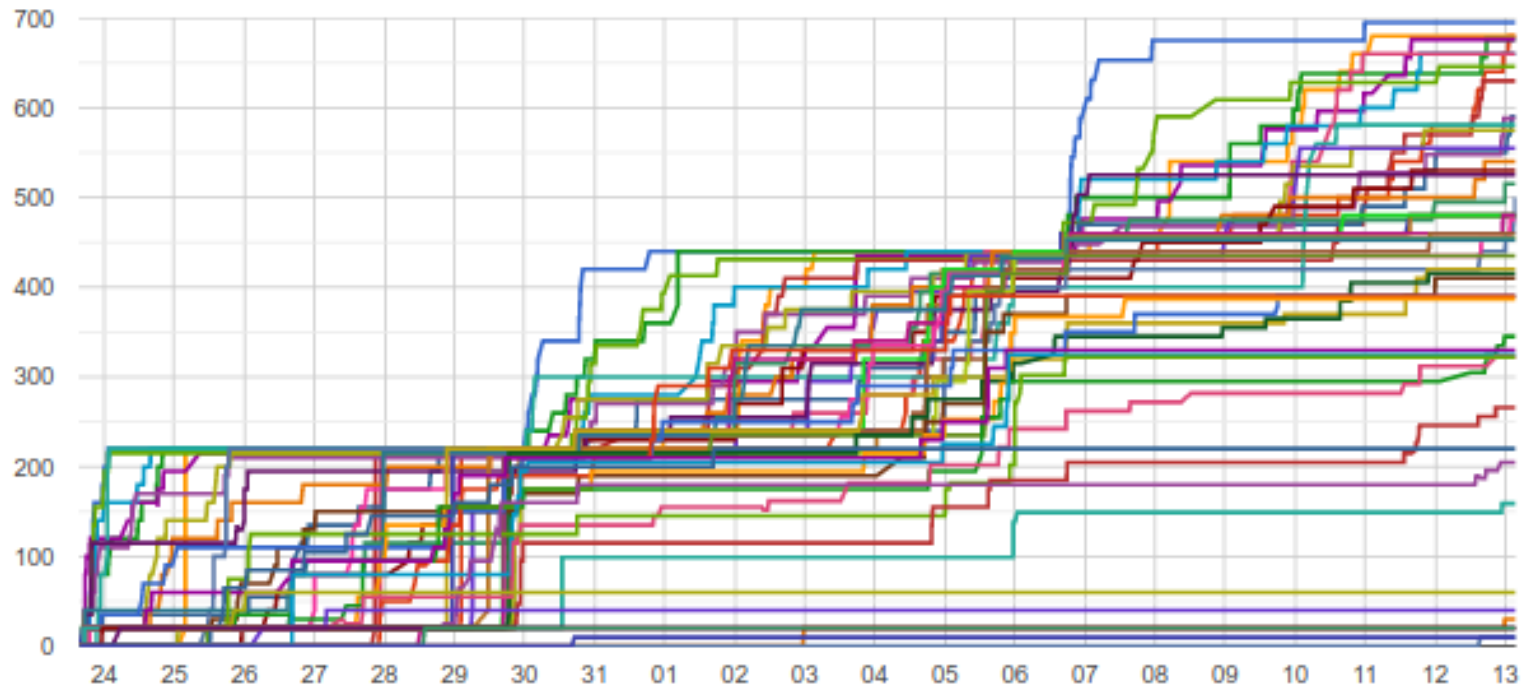


Lec04: Writing Exploits

Taesoo Kim

Scoreboard



Administrivia

- Please join [Piazza](#)
- Two optional recitations on every Mon/Wed (check piazza)!
- **Due** : Sept 19th at midnight (**2 weeks**)
- **In-class CTF** : Nov 22–Nov 23!

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  
7fffffffde000-7fffffff000 rw-p 00000000 00:00 0 [stack]
```

```
$ cat /proc/self/maps | grep stack  
7fffffffde000-7fffffff000 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
```

```
...
```

```
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

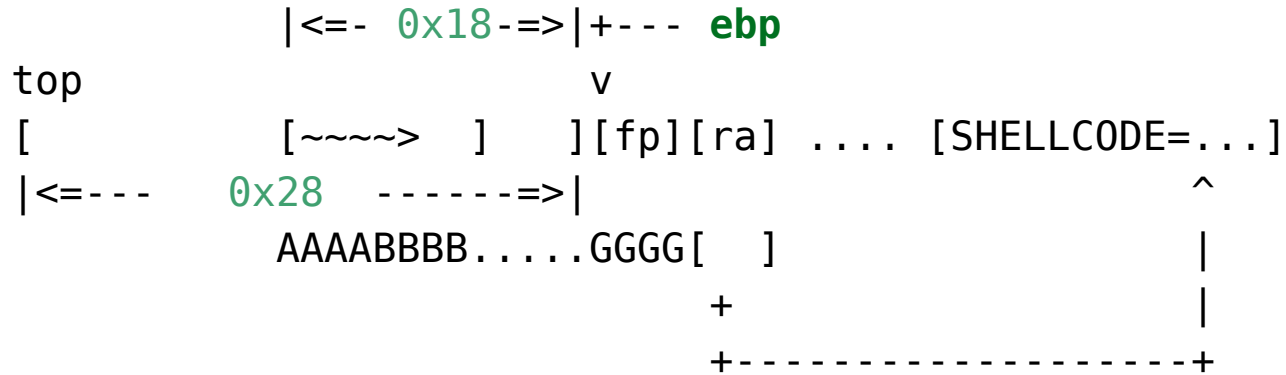
```
top          |<=- 0x18 -=>|+--- ebp
              v
[           [~~~~> ]  ][fp][ra]
|<=--- 0x28 -----=>|
          AAAABBBB.....GGGGHHHH
```

Where to put Shellcode?

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

Example: Injecting Shellcode (e.g., 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@3.223.237.92  
Password: <password>
```

```
$ cd tut03-pwntool  
$ cat README
```

References

- [Phrack #49-14](#)