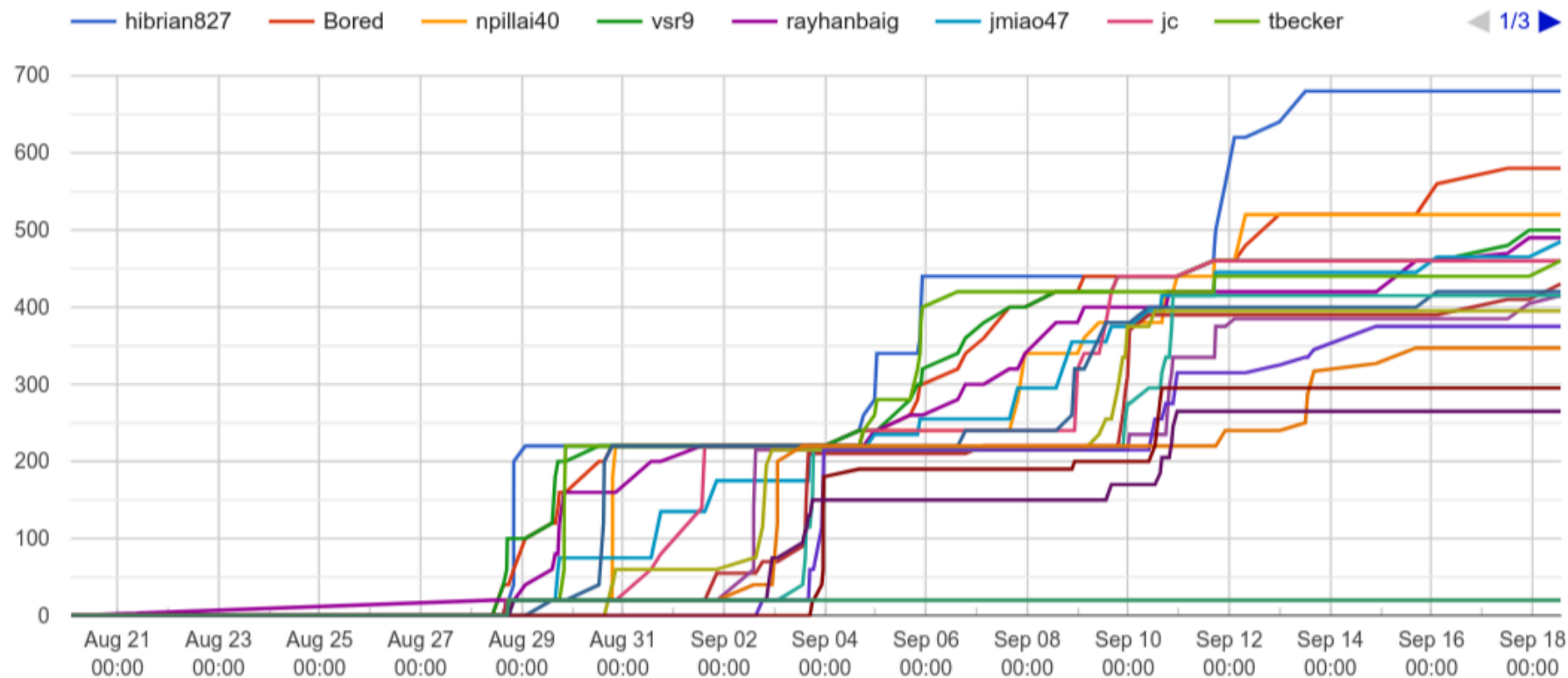


Lec04: Writing Exploits with Pwntools

Taesoo Kim

Scoreboard



Administrivia

- Please join [Ed](#)
- Optional recitations: Tue/Wed (@Coda)
- **Due**: Sep 24 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
```

```
7fffffffde000-7fffffffff000 rw-p 00000000 00:00 0 [stack]
```

```
$ cat /proc/self/maps | grep stack
```

```
7fffffffde000-7fffffffff000 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 -M intel -d crackme0x00
```

```
...
```

```
080492b3 <start>:
```

```
80492b3: 55
```

```
push ebp
```

```
80492b4: 89 e5
```

```
mov ebp, esp
```

```
80492b6: 83 ec 10
```

```
sub esp, 0x10
```

```
...
```

```
|<=- -0x10 ==>|+--- ebp
```

```
top v
```

```
[buf .. ][fp][ra]
```

Reminder: crackme0x00

```
$ objdump -M intel -d crackme0x00
```

```
...
```

```
80492d3: 8d 45 f0
```

```
lea    eax, [ebp-0x10]
```

```
80492d6: 50
```

```
push   eax
```

```
80492d7: 68 59 a0 04 08
```

```
push   0x804a059
```

```
80492dc: e8 af fd ff ff
```

```
call   8049090 <__isoc23_scanf@plt>
```

```
...
```

```
|<=- -0x10 ==>|+--- ebp
```

```
top          v
```

```
[~~~~~>      ][fp][ra]
```

Reminder: crackme0x00

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

Reminder: crackme0x00

```
|<=-  -0x10 -=>|+--- ebp  
top          v  
[~~~~~>     ][fp][ra]  
AAAABBBBCCCCDDDDDEEEFFFFF
```

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?

```
|<=-  -0x10 -=>|+--- ebp
top          v
[~~~~~>      ][fp][ra] .... [SHELLCODE=...]
AAAABBBBCCCCDDDDDEEEE[  ]      ^
                        +        |
                        +-----+
```

In-class Tutorial

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

```
$ ssh lab03@52.201.10.159  
Password: xxxxxxxx
```

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

References

- [Phrack #49-14](#)