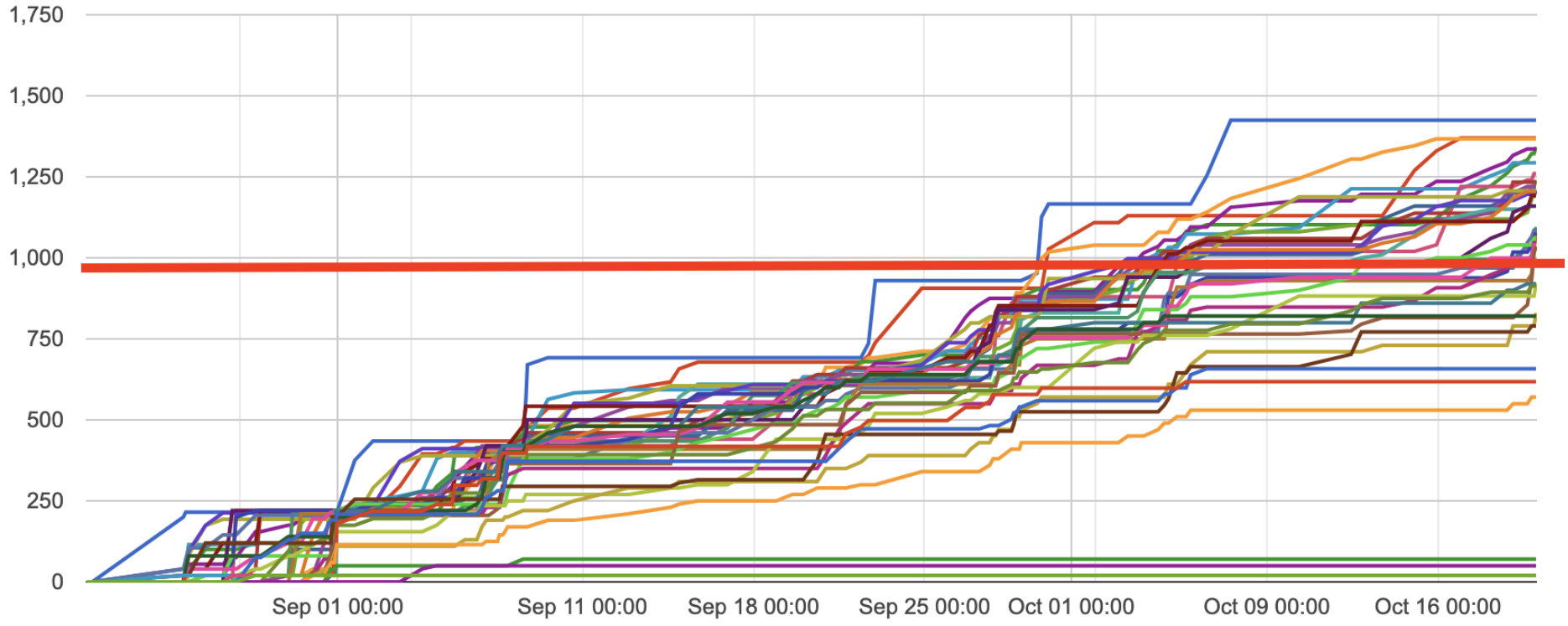
Lec09: Remote Exploit

Taesoo Kim

Scoreboard


1,750
1,500
1,250
1,000
750
500
250
0
Sep 01 00:00
Sep 11 00:00
Sep 18 00:00
Sep 25 00:00
Oct 01 00:00
Oct 09 00:00
Oct 16 00:00

Note on Score/Grade

- 160 per lab x 6 labs = 960 for A
- So far, except 9, all A
- If you want to get A, there are plenty of other options:
  - NSA Codebreaking challenges
  - Solving old labs/challenges (50% penalty)
  - Piazza participation
  - Win TKCTF!

Administrivia

- In-class CTF: https://ctf.gts3.org/ (Open to public! Dec 01)
  - Registration: http://bit.ly/tkctf_register (#2-3 persons per team)
  - Rules: https://tc.gts3.org/cs6265/2023-fall/ctf.html
  - Submit your team's challenge by Nov 27
- NSA Codebreaker Challenge → Due: Dec 08

Summary of Lessons so far

- Lab01/02: Reverse engineering, shellcode writing
- Lab03: Stack overflow
- Lab04: Stack canary, shield, shadow stack, etc to prevent stack overflow!
- Lab05: DEP/ASLR to make it even harder to exploit (Q. fmtstr?)
- Lab06: ROP to break even when all combined

→ But all in *local* environments (i.e., local privilege escalation)

Summary of Lab06

- Powerful computation w/ ROP
  - **puzzle**: arbitrary string
  - **rop-sorting**: arbitrary computation
- ROP gadgets
  - **pop**: subtlety of CISC (an immediate operand)
  - **upto-retaddr**: pivoting stack
  - **find-gadget**: even from compiler-supplied code
- Attack vector
  - **fmtstr-relro** (under RELO), **sprintf**, **inc1**

Remote Challenges

- Use techniques learned from Lab01-Lab06
- But targeting the remote server (e.g., online services)!

In-class Tutorial

- Step1: nc
- Step2: brute force attack
- Step3: guessing attack
- Step4: crackme0x00 in a remote setting (tut02)

```
$ ssh lab07@54.88.195.85
Password: <password>

$ cd tut07-socket
$ cd tut07-remote
```