[j00ru] Filesystem (PWN 250)

first blood: **Teamless**
solved **5** times

- Linux ELF x64 executable, PIE, NX, RELRO enabled.
- Local file operations: read, write, seek
  - No "flag" allowed in filename.
  - Only operations on /dev/null and /dev/urandom actually succeed.
- Internally: a path→fd cache with 16 entries, to avoid multiple open() calls.
  - The number of operations performed on each path is also counted.

[j00ru] Filesystem (PWN 250)

first blood: **Teamless**
solved **5** times

- Cache flushing
  - When 16 entries are exceeded, the cache is flushed.
  - All fds are closed.
  - All cache entries are removed, except potentially one "hot file" (#usages > cumulative #usages of all other files).
- Results in a dangling fd assigned to a path.
  - Can be reassigned to any other valid path by opening another file.
  - Effectively a Use-After-Close condition on files.

[j00ru] Filesystem (PWN 250)

first blood: **Teamless**
solved **5** times

- Exploitation process:
  - Use the UAC bug to read /proc/self/maps and read the process base address.
  - Use the UAC bug again to open /proc/self/mem.
  - Seek to the address of some code in .text (e.g. loop in `main()`).
  - Write shellcode there and have it executed.
  - List the current directory and cat the flag from `find_the_flag_here.txt`.

[j00ru] Filesystem (PWN 250)

first blood: **Teamless**
solved **5** times

DrgnS{Use_4ft3r_cl0se_1s_a_c0ol_cl4ss_isn7_1t}