solved 1 time

[j00ru] Entree (pwn 250)

- Windows 32-bit challenge running on Windows Server 2012, DEP and ASLR enabled.
- Reverse echo server:
  - Loads uint32 data size (N).
  - Allocates a buffer if `N <= 0x10000`, loads bytes into it in reverse order (starting from the end).
  - Prints the buffer out using `printf()`.

[j00ru] Entree (pwn 250)

- First stage: trivial information disclosure using the format string bug.
  - Can leak the image base and stack address in one shot.
  - The %n marker is disabled on Windows by default, so writing is not possible.
- If `N > 0x10000`, the buffer pointer is NULL.
  - The code starts writing from `&buffer[N]` downwards, which means an absolute arbitrary write in the case of `NULL[N]`.
  - The loop would eventually crash trying to write to unmapped memory, but there is an exception handler which allows one exception to occur, and restarts execution at `main()`.

[j00ru] Entree (pwn 250)

- The arbitrary write can be used to write a ROP chain directly to the stack, where the second `main()` returns.
- The executable is 81kB long, has reasonably many gadgets and imports all required functions.
- Our ROP was a bit convoluted (~50 dwords), but boils down to `CreateFile() + ReadFile() + GetStdHandle() + WriteFile() + Sleep() + ExitProcess()`.
- Flag: **`DrgnS{NULl_p7r_d3r3f3r3Nc35_N07_4LL_7H47_H4RmL355}`**