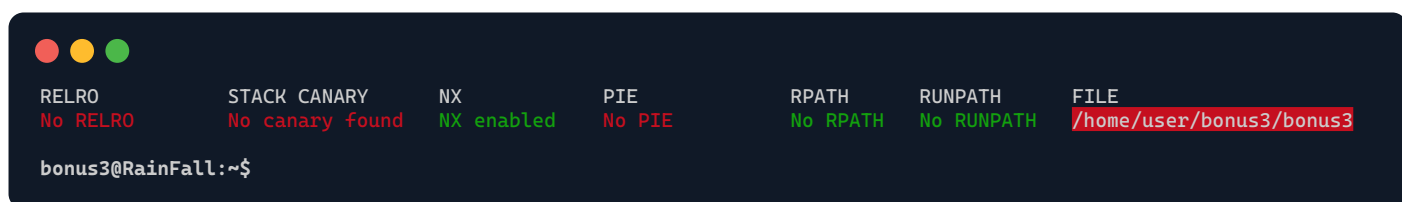
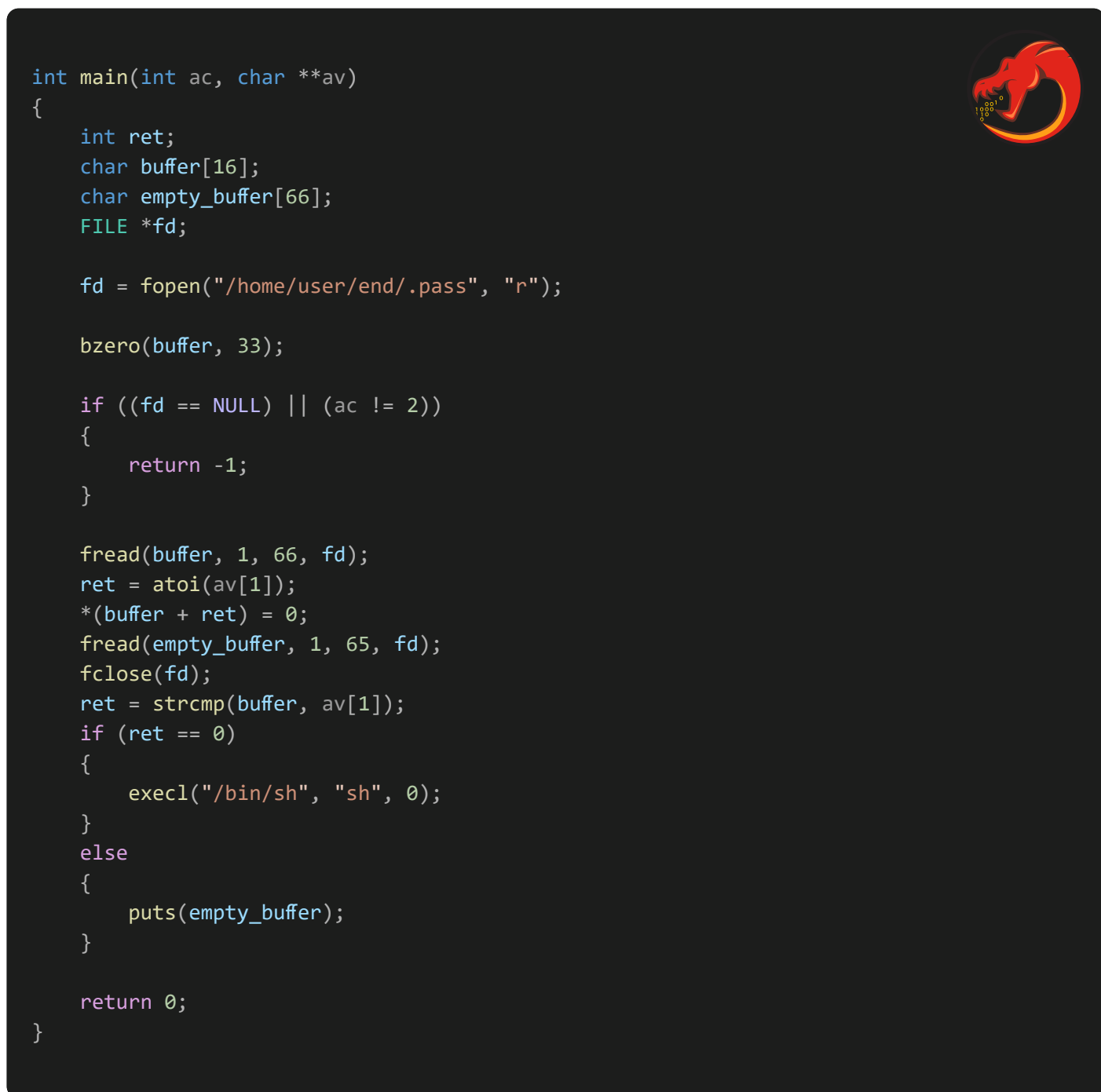


./bonus3



Decompiled file with *Ghidra*:



Upon examining the C code, it becomes clear that for the shell to be spawned, `ret` must be set to 0.

```
ret = strcmp(buffer, av[1]);
```

This means our `av[1]` needs to match `buffer`.

```
fread(buffer, 1, 66, fd);
```

The `buffer` holds 16 bytes from the `.pass` file. To access the shell, `av[1]` should match these, but they're unknown to us. Moreover, even if known, another line complicates it:

```
ret = atoi(av[1]);
*(buffer + ret) = 0;
```

If `av[1]` matches the 16 bytes from `.pass`, then `atoi` could overflow, causing the `'\0'` to be written at an out-of-bounds location, leading to a *segmentation fault*.

But, what's interesting, is that the buffer is *null-terminated* based on the result of `atoi(av[1])`.

Indeed, without knowledge of the buffer content, and considering that knowing wouldn't benefit us, our objective becomes clear: ensure both the `buffer` and `av[1]` are **identical**.

Consequently, setting both `buffer[0]` and `av[1]` to **0** is the logical solution.

To achieve this, we can provide the program with any of the following arguments: `""`, `$'\0'`, `$'\x0'`

