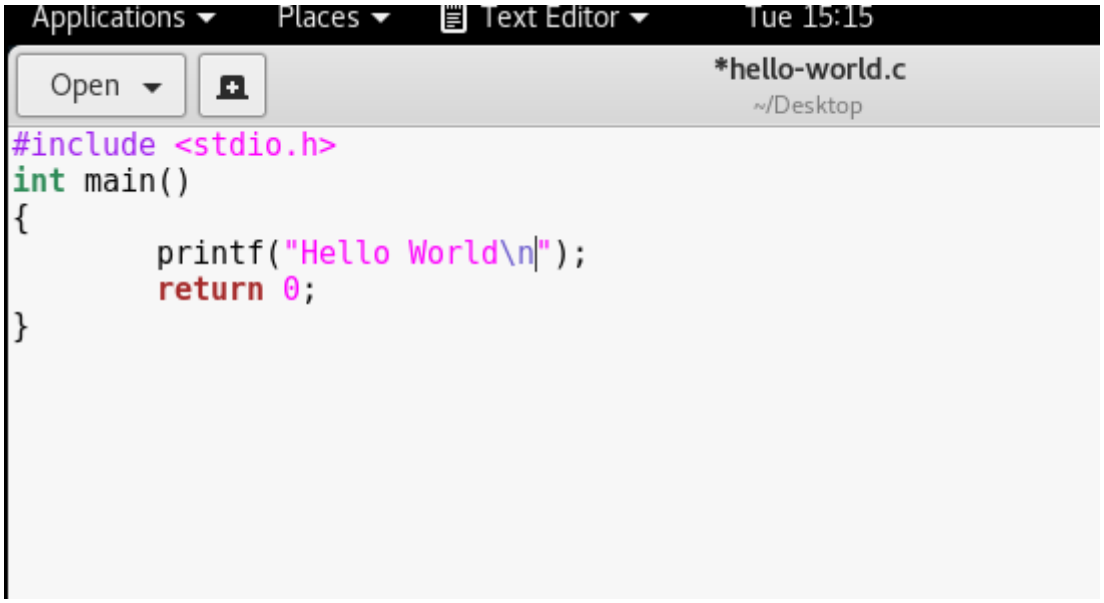
Radare2 یک فریم‌ورک متن‌باز[1] است که برای مهندسی معکوس[2] مورداستفاده قرار می‌گیرد.

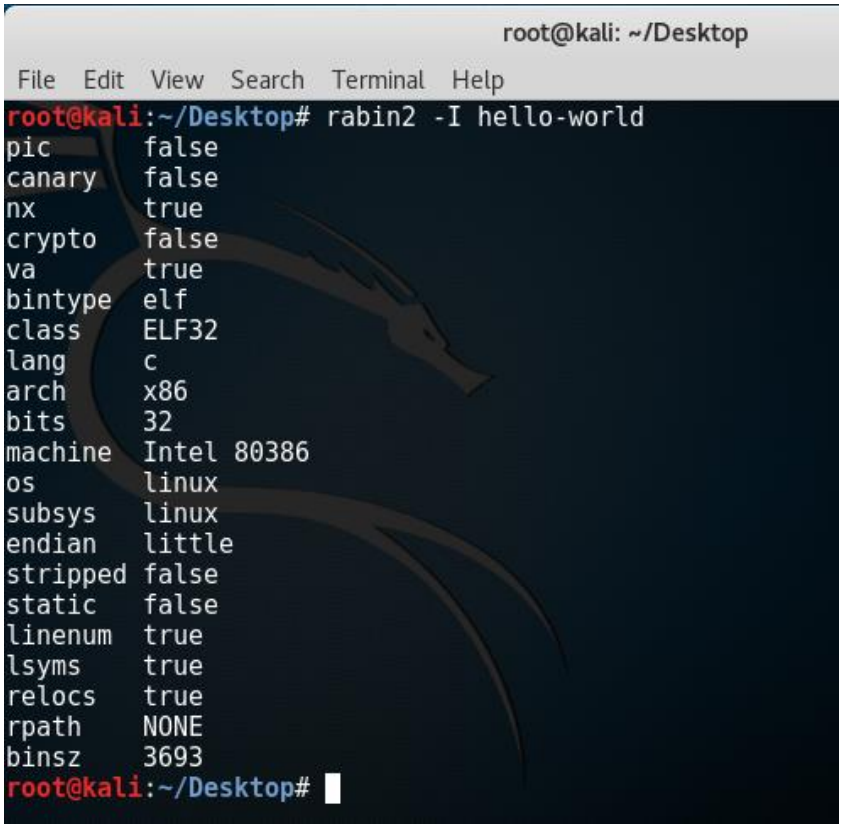
ابتدا یک برنامه‌ی hello world به زبان c می‌نویسیم:



این برنامه را کامپایل کرده و اجرا می‌کنیم تا خروجی Hello World به ما نمایش داده شود:

Rabin2 یکی از ابزارهایی است که برای به دست آوردن اطلاعات در مورد یک فایل باینری مانند string ها، زمان کامپایل و اطلاعات مفید دیگر می‌تواند مورداستفاده قرار گیرد. ما نیز از این ابزار استفاده می‌کنیم تا اطلاعاتی در مورد این برنامه به دست بیاوریم. آپشن I– اطلاعات مهم در مورد این فایل باینری را در اختیار قرار می‌دهد:

[1] Open source
[2] Reverse engineering

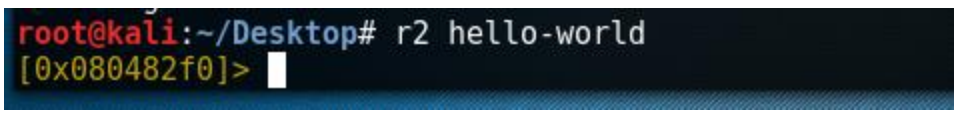


خروجی این دستور نشان می‌دهد که این برنامه روی لینوکس اجرا می‌شود و با زبان C نوشته شده است.

دستور rabin2 –z همه‌ی string های data section این فایل باینری را نشان می‌دهد:

همان‌گونه که مشاهده می‌کنید این برنامه یک string دارد: "Hello World".

حال به سراغ radare2 می‌رویم تا کد اسمبلی برنامه‌ی خود را مشاهده کنیم. با دستور زیر برنامه‌ی خود را در radare2 ، load کرده و وارد محیط radare2 می‌شویم:



گام بعدی این است که به radare2 اجازه دهیم تا این فایل باینری را آنالیز کند و اطلاعاتی مانند string ها، توابع و اطلاعات مهم دیگر را از آن استخراج کند. بدین منظور دستور aa را اجرا می‌کنیم:

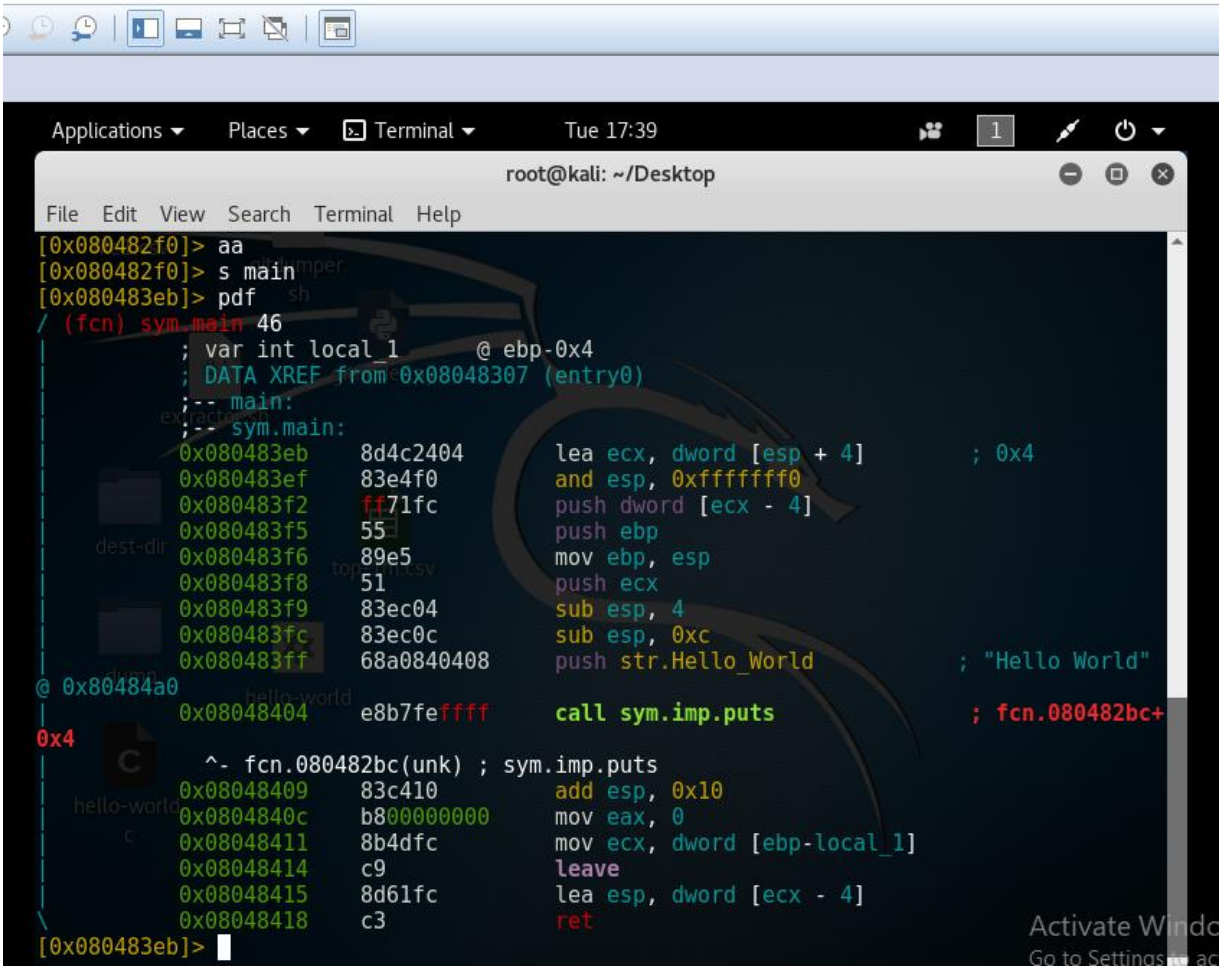
```
root@kali:~/Desktop# r2 hello-world
[0x080482f0]> aa
```

دستور s در radare2 برای جستجوی نقطه‌ی مشخصی از حافظه استفاده می‌شود که میتوانیم یک آدرس هگزادسیمال یا اسم یک تابع را به آن بدهیم. ازآن‌جا که اکثر برنامه‌های لینوکس با تابع main آغاز می‌شوند ما به دنبال تابع main می‌گردیم:

```
[0x080482f0]> s main
[0x080483eb]>
```

همان‌گونه که مشاهده می‌کنید آدرس از 0x080482f0 به 0x080483eb تغییر کرد. این به این معنا است که ما اکنون در تابع main هستیم و آدرس کنونی ما 0x080483eb است.

با دستور pdf (print disassembly function) می‌توانیم کد این تابع (تابع main) را مشاهده کنیم:



همان‌گونه که مشاهده می‌کنید در این تابع رشته‌ی "Hello World" در آدرسی از حافظه قرار می‌گیرد و سپس تابع sym.imp.pus فراخوانی می‌شود که این تابع رشته‌ی موردنظر ("Hello World") را چاپ می‌کند و نهایتاً با ret تابع به پایان می‌رسد.

بنابراین ما بدون اینکه این برنامه را اجرا کنیم متوجه شدیم که این برنامه رشته‌ی "Hello World" را چاپ می‌کند.