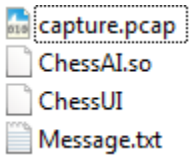
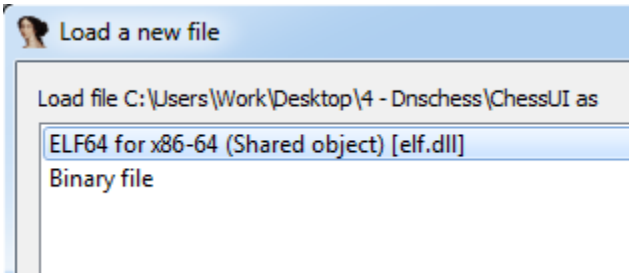
Dnschess

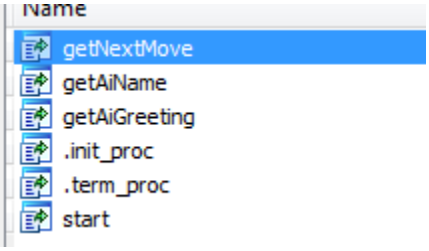
Challenge này bao gồm các file



Mở ChessUI bằng IDA Pro ta thấy đây là 1 chương trình chạy trên Linux:



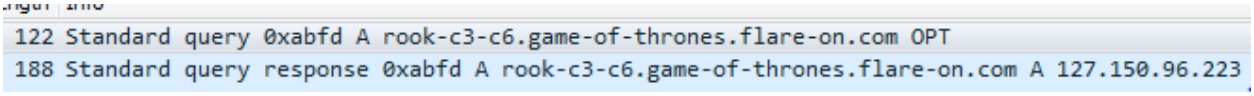
Sau khi kiểm tra xong ChessUI thì thấy nó load thêm ChessAI.so, check ChessAI.so ta thấy có các export:



Kiểm tra hàm getNextMove ta thấy:

```
start = a3;
end = a4;
v8 = a5;
v12 = __readfsqword(0x28u);
strcpy(&dest, chessName);
sub_1145(&dest, start);
sub_1145(&dest, end);
strcat(&dest, ".game-of-thrones.flare-on.com");
v9 = gethostbyname(&dest);
if ( !v9 )
  return 2LL;
v10 = *v9->h_addr_list;
if ( *v10 != 127 || v10[3] & 1 || a1 != (v10[2] & 0xF) )
  return 2LL;
```

Thấy có hàm gethostbyname, ta mở file capture.pcap xem thì thấy:



Từ đó có thể đoán được khi đi các bước cờ thì sẽ trả về một ip, ip đó dùng để check xem nước cờ có hợp lệ không bằng đoạn code sau:

```
if ( *v10 != 127 || v10[3] & 1 || a1 != (v10[2] & 0xF) )
  return 2LL;
```

Nếu:

- IP network không phải 127.xxx.yyy.zzz
- zzz là số lẻ
- yyy & 0xF không bằng a1, ở đây sau khi phân tích thì a1 là số thứ tự nước đi hiện tại

Thì bạn sẽ thua bàn cờ và không lấy được Flag

Đến đây, chúng ta build một local DNS trên linux để chạy bàn cờ này và dựa theo thứ tự các nước đi như sau để lấy được flag:

```
pawn-d2-d4.game-of-thrones.flare-on.com   127.53.176.56
pawn-c2-c4.game-of-thrones.flare-on.com   127.215.177.38
knight-b1-c3.game-of-thrones.flare-on.com   127.159.162.42
pawn-e2-e4.game-of-thrones.flare-on.com   127.182.147.24
knight-g1-f3.game-of-thrones.flare-on.com   127.252.212.90
bishop-c1-f4.game-of-thrones.flare-on.com   127.217.37.102
bishop-f1-e2.game-of-thrones.flare-on.com   127.89.38.84
bishop-e2-f3.game-of-thrones.flare-on.com   127.230.231.104
bishop-f4-g3.game-of-thrones.flare-on.com   127.108.24.10
pawn-e4-e5.game-of-thrones.flare-on.com   127.34.217.88
bishop-f3-c6.game-of-thrones.flare-on.com   127.25.74.92
bishop-c6-a8.game-of-thrones.flare-on.com   127.49.59.14
pawn-e5-e6.game-of-thrones.flare-on.com   127.200.76.108
queen-d1-h5.game-of-thrones.flare-on.com   127.99.253.122
queen-h5-f7.game-of-thrones.flare-on.com   127.141.14.174
```

Và sau khi đi xong bàn cờ ta có flag là: