Computer Security HW0x5

R08946007 資科所 蔡昀達

Nickname : r08946007

Casino

1. 首先觀察 source code 可以發現使用的變數存在 global，因此先把這些變數位置找出來

   0x00000000006020b0 lottery
   0x00000000006020d0 guess
   0x00000000006020f0 name
   0x0000000000602100 seed
   0x0000000000602104 age
2. 觀察 source code 發現可以任意寫記憶體的地方

   line51 : guess[idx] = read_int();
3. 觀察 source code 發現 read(0,name,0x100)會 overflow，可以輸入 0x100 個 byte
4. 通靈許久後終於發現可以 got hijack，因此先用 objdump 找到 got table 存放各涵式的位置
5. 綜合以上擬訂策略:
   1. 將 shellcode 放在 name 變數
   2. 因為 name 會 overflow 覆蓋到 age 的位置，因此輸入 age 必須要保持 shellcode 的完整性
   3. 因為 puts 涵式剛好會先呼叫到一次，因此將 got table 的 puts 位置蓋成 name 的位置，也就是 guess[-44]的位置，在第二次回圈時覆蓋成功後進入 guess=lottery 可以呼叫第二次 puts
   4. 在 guess[idx] = read_int(); 複寫記憶體時 因為只能寫 4byte 因此必須複寫兩次才能覆蓋完整