Computer Security Homework 0x01

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

Back To The Future

Part 1. 靜態分析

一開始拿到這隻程式, 將它先執行起來, 發現要輸入密碼, 隨便輸入密碼後它會輸出一個奇怪的 flag, 顯然不是真正的 flag。 於是把它丟到 Ida Pro 看看能不能 decompile, 試了結果發現它可以。

觀察了一段時間之後就大概知道程式流程是如何了,

1. 將目前年份讀到一個變數當中 (姑且稱之為 year)
2. 輸入一組密碼 (password)
3. 將 password 所有的 element 與 0x20 進行 or 的操作 assign 到新的 password
4. 將 password 所有的 element 與某個運算 (可能跟 year 和 machine guard 有關) 的結果進行 xor 然後跟一個 array (key1) 的對應的 element 比較, 如果不一樣就會跳出迴圈, 如果能夠跑完此迴圈就能夠保證此時的 password == key1
5. 將 password 的每個 element 和另外一個 array (key2) 的對應的 element 進行 xor 操作存回原本的位置
6. 將 password 的內容輸出為 flag

由此可知, 不妨可以試試看用 key1 和 key2 的每個對應的 element 都 xor 試試看結果會如何, 在 Ida Pro 可以找到這兩個 array 的內容, 然後用 python xor 就可以得出結果, 還真的得到 flag 了。

Part 2. 動態分析

因為這題還是要輸入正確密碼才會輸出正確的 flag, 用動態分析就可以更清楚知道程式運行的流程, 用動態分析的作法便是將程式用 x64dbg 動態去更改裡面的 data 和 registers, 最終輸入正確的密碼, 就會輸出正確的 flag。

程式執行開始之後首先會輸出一些訊息, year 若不是 1985 就會跳出 warning, 索性就把 year 設為 2019 的地方下 breakpoint, 在 x64dbg 觀察到的 assembly 如下,

```
004016E3 | A3 40C04000            | mov dword ptr ds:[40C040],eax            |
```

然後把 `eax` 值設為 1985, 接著它會跳出 `[!] Time Machine Guarder:` 是 `SAFE`, 抑或是 `HARMFUL`, 取決於以下三行

```
00401715 | 8B45 E0                | mov eax,dword ptr ss:[ebp-20]            |
00401718 | 0FB640 02              | movzx eax,byte ptr ds:[eax+2]            |
0040171C | 84C0                   | test al,al                               |
```

將 `ebp-20` 所指到的位置得出來 (每次都不一樣), 然後將它 +2 byte 的值改為 0, 就可得到 `[!] Time Machine Guarder: [SAFE]` 的訊息。

接著先隨意輸入一組 password, 拜靜態分析所賜, 我知道之後會有一個 for 迴圈, 它會進行 `2*(1985+63) + 0 + 127`, 將結果 (0x107f) 和 password xor 存為新的 password, 然後和 key1 比較是否相等, 因為一個一個動態改 password 的 element 太麻煩了, 不妨就用 python 把 key1 (keychecker.408008), 在 x64dbg 上看到的 dump 如下,

```
00408008  1D 13 10 18 51 4C 4F 1C 12 51 0B 08 50 51 50 51  ....QLO..Q..PQPQ
00408018  50 51 50 00 5B 5F 51 5F 2A 1C 0A 43 33 02 54 4D  PQP.[_Q_*..C3.TM
```

當中的 1D 13 10 ... 50 51 50, 19個 byte 分別和 0x7f xor, 就可以得到 password 為 `blog.30cm.tw/./././`, 再重新執行一次, 動態把 year 改為 1983, time machine guarder 讓它 safe, 將此密碼輸入到 console, 就可以得到真正的 flag。