[hw0x04] writeup

莊翔旭, woolninesun, b04902083

De-de-deobfuscation

1. 先算出 payload 要多長才會蓋到 return address，用 gdb trace 到 memcp 後面的位置找到第一次輸入的 buffer 位置，算出 payload 長度為 0x148
2. 隨後發現直接用 'A'*0x148 的 payload 會在 bytestostring 的地方出錯，所以要構造不會出錯的 payload，最直接的方式是使用 x/41gx dump 整個 buffer，先去比對兩臺機器 dump 的結果，發現都一樣，表示可以直接將 dump 出來的結果做 payload 之後在後面加上 ROP chain。
3. ROPchain 的方式寫在 script 的 comment 裡！