Introduzione

"L'analisi di un sistema allo scopo di identificarne le parti costitutive e le loro inter-dipendenze per creare una nuova rappresentazione del sistema stesso o comunque una sua visione ad un più alto livello di astrazione; il Reverse Engineering viene spesso impiegato per intervenire su sistemi per i quali non si ha accesso al design originale."

FOLDOC dictionary — by Denis Howe

Ok, questa è la definizione scritta sui libri, ma in realtà rappresenta qualcosa che va ben oltre il semplice "saper smanettare con il PC"; è qualcosa che è più giusto ricondurre ad una sorta di modus operandi generico che è possibile applicare ad ogni "sistema" reale...

Secondo il mio (modesto) parere, il Reversing è un'espressione della curiosità insita nell'uomo di guardare oltre il "primo strato", la sua necessità latente di scoprire come funzionano le cose che ci stanno intorno, dal frigo della cucina alla centrale nucleare; il desiderio di conoscere i meccanismi interni per modificarli a nostro piacimento: in sostanza, l'espressione della volontà di imparare cose nuove, andando più a fondo di un semplice approccio superficiale.

Quando si "reversa" qualcosa, lo scopo principale è quello di ottenere più informazioni possibile sul nostro target, capire e cercare di prevederne le mosse a nostro favore; ecco perché il reverse engineering è spesso applicato al software, uno dei più grandi contenitori di informazioni che l'uomo ha a disposizione. Avete mai pensato che tutti i programmi in fin dei conti sono soltanto una miriade apparentemente casuale di bits che ha senso solo se interpretata nel modo giusto?

Manipolare effettivamente un programma è facile, ma non è affatto semplice sapere dove si devono mettere le mani, quindi possiamo farci aiutare dallo stesso ambiente in cui "vive" il target: la scatola degli attrezzi che possiamo avere a disposizione è anch'essa composta da software che ci servirà durante la nostra chirurgia informatica; vi assicuro che arrivare ad avere in pugno la creatura di un programmatore è una sensazione difficile da descrivere, ma molto particolare ed in un certo senso appagante...

Alla fine uno potrebbe anche pensare che questi siano i soliti discorsi da nerd fissati con i computer, per i quali nel mondo non esiste altro che uno schermo ed una tastiera, ma non è così: l'informatica è una scienza molto teorica e rigorosa, ma, se affrontata da un altro punto di vista, può facilmente coinvolgere un sacco di discipline apparentemente eterogenee: matematica, logica, giochi, creatività e, perché no, anche un po' di fantasia...

(in basso, un programma sotto gli occhi vigili di IDA...)