Tutorials

Quando ho cominciato anch'io da "niubbo" non sapevo dove sbattere la testa; sì, ok, la teoria l'avevo studiata e più o meno sapevo dove andavo a parare, ma “tra il dire ed il fare c'è di mezzo "e il"...” (Elio e le Storie Tese). Ben presto ho realizzato che la cosa migliore era cominciare a mettere in pratica, quindi dopo aver raccattato un po' di tools a destra e a manca, ho cominciato a leggermi qualche tutorial trovato in rete...

Il primo che ho letto è stato "Ancient Art of Cracking" di Buckaroo Banzai, che mi ha veramente aperto gli occhi; poi sono incappato nei mitici tutorials di Old Red Cracker, membro dell'allora foltissima schiera di adepti di Fravia, un altra eminenza fra i pionieri del cracking su PC (questo mirror è quello che rimane del suo glorioso sito... ora si è dato alle ricerche sul Web, che spreco...).

Erano altri tempi... si parla del 1995 circa; c'era ancora molto da scoprire e chi rompeva per primo una protezione si guadagnava l'ammirazione ed il rispetto della Scena. Le BBS ribollivano di hacker e la gente si arrangiava con quello che aveva, e spesso bastavano il DEBUG e l'EDIT del DOS!

Oggigiorno siamo andati molto avanti con il software ed esistono strumenti in grado di analizzare i programmi fino al midollo, quindi la bravura del reverser moderno risiede piuttosto nell'intuizione e nell'esperienza, più che nella perizia tecnica e le ossa ci si fanno appunto provando e riprovando, sperimentando le varie tecniche senza mai porsi limiti e cercare sempre di usare al meglio la nostra arma più forte: l'intelligenza.

Come per le guide sull'assembler e compagnia bella, sul sito della UIC troverete di tutto di più, oltre a numerosi tutorials sui target più disparati; Quequero è stato così gentile da ospitare i miei tutorials, di cui riporto i links qui sotto... se avete voglia, leggeteli e provateli:

{ se trovate errori od imprecisioni, comunicatemelo che provvederò ad aggiornarli quanto prima. }

-

Tutorials completi:

- L8+ 5.2.8 reversing - (24/04/2004) - [mirror]

- SOARP Crackme - (26/06/2004) - [mirror]

- KeygenMe 2 - (12/09/2004) - [mirror]

- PTGui 4.1 reversing - (25/03/2005) - [mirror]

- Keygen 1° Corso studenti UIC - (12/09/2005)

-

“Mini-Tutorials” (nati durante le discussioni sul Forum)

-

Reversing di 0-Code HTML Converter - (04/12/2004)

-

Reversing di Neutrino through Windows - (12/12/2004)

-

Procedura generica per il Manual Unpacking - (10/02/2005)

- Cenni sul Keygen Injection - (11/02/2005)
- Reversing di Gestione Condomini - (22/02/2005)
- Reversing di Visual Business Card 4 - (02/03/2005)
- Estrazione di un'immagine da un eseguibile Delphi - (08/04/2005)
- Reversing di Softvision BigRace - (30/04/2005)
- Patching di GMFC 2.2 - (23/08/2005)
- Patching di PacTerm 3.0 - (08/09/2005)
- Patching di Pdf2Word [parte 1 e 2] - (14/10/2005)

Guest Tutorials:

- Reversing completo di Leonardo - (autore: DaGoN)
- Crackme in Java [tutorial + sources] - (autore: DaGoN)
- Armadillo 3.xx-4.xx unpacking [in spagnolo] - (autore: Tk0017)

Girellando qua e là su internet si trovano moltissimi siti di tutorials dalla qualità molto eterogenea, quindi ho pensato di fornirvi una piccola lista di fonti di tutorials abbastanza consolidata:

The Krobar Collection (immenso repository di tutorials raccolti da centinaia di fonti!)

ARTeam Tutorials (il mirror di tutti i tutorials dell'ARTeam, aggiornati al 13/06/2005)

RCE Forum (un forum con tutto ciò che riguarda il Reversing... ovviamente non è niente paragonato alla UIC...)

Woodmann Crackz è il sito relativo al forum sopra citato (non troppo organizzato, ma pieno di tutorials e tools)
ToTheSky.us contiene parecchi tutorials sul manual unpacking (adesso sembra down, ma spero che funzioni presto)
Il sito di pinc0pall è una miniera di tutorials, complimenti per l'impegno e la pazienza nel raccoglierli tutti!