

# Prefazione all'edizione italiana

Alla fine del 2003 ero rimasto molto colpito di fronte al preview della prima edizione del libro che avete tra le mani. Apogeo mi aveva chiesto di esprimere un parere, parere che pagina dopo pagina si concretizzava in maniera più che positiva, al punto che più che volentieri accettai di scrivere la prefazione a *L'arte dell'hacking* e molte volte mi ritrovai in seguito a consigliare il libro a chi mi contattava per avere consigli e informazioni sulle basi di quello che potremmo chiamare “serious hacking”.

Sono passati circa quattro anni, ed eccomi di nuovo alla prese con il libro di Jon Erickson. Eccomi di nuovo a confermare quanto già scrissi ai tempi. Eccomi di nuovo conquistato dal lavoro di Jon, quasi raddoppiato come numero di pagine in questa seconda edizione.

Ancora una volta sorrido con piacere (ri)leggendo nei ringraziamenti come “tutto sia iniziato” con il Commodore VIC-20 regalo dei genitori: quanti amici della comunità hacker hanno un ricordo simile?

Ancora una volta non posso che condividere e approvare il pensiero alla scena underground senza la quale molto di quello che state per leggere non potrebbe esistere.

La pubblicazione di libri come questo è importante. Certo, con quasi 500 pagine non è più possibile affermare di essere di fronte a un testo agile, ma basta scorrere l'indice per capire come la struttura sia quanto mai compatta e profonda: pochi argomenti chiari, precisi e soprattutto dettagliati.

La seconda edizione di *Hacking – The Art of Exploitation* (continuo a preferire il titolo originale) include inoltre un CD-ROM, ma non aspettatevi di trovarci gli hacking tool del momento, bensì il codice sorgente del libro e un ambiente (una distribuzione live GNU/Linux Ubuntu) ottimizzato per lo sviluppo di exploit.

Perché lo spirito è proprio questo: non tanto imparare come utilizzare i tool di attacco ed exploiting, bensì comprendere lo spirito e la teoria della scienza che sta dietro alla pratica dell'hacking.

Per essere più chiari, qui imparerete i concetti grazie ai quali potrete iniziare a scrivere da soli i tool e comprenderne le logiche. Questo grazie a esempi pratici, codice da utilizzare come base, idee e suggestioni, che sebbene non rappresentino di per sé nulla di “rivoluzionario”, sono un punto di partenza per costruire, crescere, imparando a conoscere se stessi e le diverse modalità che esistono per affrontare – e risolvere – i problemi.

La massima che imparerete dalla lettura che state per iniziare si può, forse, riassumere così: che siate blackhat o che siate whitehat, apprezzerete i concetti di “pensare out of the box” propri di questo libro, che si parli di creare un exploit unreleased, o che si affronti l'argomento di come proteggere un sistema o un'applicazione da attacchi multilivello. L'idea di risolvere un problema in un modo assolutamente non previsto – e non convenzionale – è probabilmente la migliore definizione che si può dare al termine hacking, ed è quello che fa (anche) la differenza tra una buona e una cattiva sicurezza nel mondo dell'ICT. Questo libro ne insegna le logiche, a voi farne buon uso. Alla faccia di chi dice che gli hacker sono tutti criminali...

*Raoul “Nobody” Chiesa  
Gennaio 2008*