

# Indice

<b>Prefazione .....</b>	<b>vi</b>
-------------------------	-----------

<b>Introduzione .....</b>	<b>ix</b>
---------------------------	-----------

Il lato oscuro dell'investigatore .....	ix
Un libro "suggerito" .....	x
E ora... i capitoli!.....	xi
Quattro chiacchiere tra amici .....	xii
Convenzioni utilizzate nel libro .....	xiii

<b>Ringraziamenti .....</b>	<b>xv</b>
-----------------------------	-----------

<b>Capitolo 1 - Due chiacchiere per iniziare .....</b>	<b>1</b>
--	----------

Si torna al lavoro .....	1
Informazioni? E cosa me ne faccio? .....	3
Cosa devi sapere .....	4
Vista? Perché Windows Vista? .....	5
Ehi, ma io ho già letto "L'investigatore informatico"! .....	6
Iniziamo? .....	6
DOS: molto arrosto e niente fumo .....	7
Online: sempre, ma non sempre .....	8
Virus: pericoli del mestiere .....	10
ZipGenius amico mio .....	11
Pronti per le indagini .....	12

<b>Capitolo 2 - Voglio il tuo Windows. O il suo .....</b>	<b>13</b>
---	-----------

Hacker, criminali, investigatori .....	13
Al di là della password .....	14
Pagare? Nun me va! .....	21
BIOS o non BIOS, questo è il problema.....	22
A mali estremi... ..	26

<b>Capitolo 3 - Ti conosco, birichino.....</b>	<b>31</b>
... quindi fai il bravo o mi arrabbio.....	31
Da cosa partiamo? .....	33
Indirizzo IP, piacere di conoscerla.....	34
Un ping per amico .....	35
Ti scoprirò!.....	39
Dalla parte del cattivo.....	40
Toc toc... crash!!! .....	44
All'opera con Nessus .....	46
Fuori il rapporto, gringo.....	52
Nmap, lo specialista delle porte.....	53
Usa Nmap, che la vita ti sorride!.....	56
<b>Capitolo 4 - È permesso? No. Fa lo stesso! .....</b>	<b>61</b>
Sapere è potere!.....	61
A te i comandi.....	62
Un capolavoro di programma.....	64
Che fare adesso?.....	76
<b>Capitolo 5 - Stop al criminale!.....</b>	<b>77</b>
Phishing: a volte serve.....	77
Falso come l'originale.....	79
Cambia faccia al sito!.....	84
Un trojan per amico.....	85
Il matrimonio s'ha da fare.....	87
Teoria poca, pratica tanta .....	91
E-mail truffaldina, che passione!.....	95
Una e-mail ad arte.....	98
Traccia senza tracce.....	100
<b>Capitolo 6 - In casa del nemico .....</b>	<b>103</b>
Una veloce scansione .....	103
Netcat, pensaci tu!.....	108
Evviva la vendemmia.....	113
Analisi dei dati (un titolo serio, per una volta) .....	116
Un'immagine vale più di mille... pacchetti.....	121
Tanti utilizzi pratici .....	125
<b>Capitolo 7 - Come 007. Anzi, di più .....</b>	<b>127</b>
Quando l'abito fa la spia .....	127
Tommi, Genualda e il terzo incomodo .....	128
Ancora più 007... ..	133
Uno sguardo ai risultati... ..	144

**Capitolo 8 - A ognuno il suo.....147**

Trucchi per veri intenditori.....	147
iPhone, che passione. Per gli altri.....	147
Spia il telefono.....	156
Dammi il verme.....	158
Trojan fai da te.....	162
Saluti e baci .....	167

**Appendice A - Porte-per-te.....169****Appendice B - Posta por...te.....175**

# Prefazione

*Matrix 2* non mi è piaciuto, *Matrix 3* non ho neppure trovato il coraggio di guardarlo e lo stesso vale per *Shrek*. Se penso a tutti gli *Squalo* dopo il primo mi viene la nausea e quando la seconda trilogia di *Guerre Stellari* non esisteva stavamo tutti meglio, credo. Magari sono strano io o sono gli esempi a essere sbagliati, ma i *sequel* proprio non mi vanno giù, specialmente se il primo episodio, l'originale, lo considero un capolavoro.

Quindi immaginatevi che cosa posso aver pensato quando mi è arrivato sulla scrivania (del computer) *L'investigatore informatico 2*, per di più con la cordiale richiesta di scrivere la prefazione, compito al quale in genere tengo moltissimo. Ho resistito all'idea di cancellare subito tutti i *file* solo perché oramai sono diventato un uomo saggio. E ho fatto bene. Proprio come quando ho deciso di guardare *Indiana Jones e il tempio maledetto* pensando che, per la maledizione del *sequel*, non mi sarebbe piaciuto. Io, addirittura, sono di quelli che si sono divertiti a vedere il quarto episodio, *Indiana Jones e il regno del teschio di cristallo*, ma questa è un'altra storia e prego l'autore di questo libro di non prenderlo come un invito a scriverne altre due puntate...

Chiudo con i paralleli cinematografici altrimenti finisco lo spazio a disposizione prima di aver chiarito la cosa più importante. Ovvero: perché mi è piaciuto il primo libro e, nonostante apparentemente sia un *sequel*, anche il secondo. La spiegazione è fin troppo semplice: sono due cose che si assomigliano poco. Diciamo che, a fare il gioco delle differenze, sono divertenti uguale, utili uguale, facili da capire uguale. Tutto uguale. Solo che l'episodio numero uno avvia gli ignari lettori ai segreti dei professionisti che indagano sui computer trattandoli come "scena del crimine", mentre l'episodio numero due, cioè questo che avete in mano, parla di come, con un po' di abilità, alcune tecniche da *hacker* possono tornarvi utili nella vita privata, quella di tutti i giorni.

Io poi non so quanta gente metta davvero in pratica quello che Riccardo insegna in maniera così appassionante, ma credo che questo sia secondario. Perché a me, personalmente, basta sapere che certe cose potrei farle per sentirmi già più sereno. Immaginare che, se mi prende il capriccio, posso sbirciare nell'iPhone della moglie che non ho, controllare attraverso il computer che il figlio (che non ho) non si sia infilato in qualche pasticcio, ascoltare quello che dicono di me i colleghi che non ho (facevo il giornalista, ma dopo aver letto il primo *Investigatore informatico* ho iniziato appunto a fare l'investigatore informatico, tenendo come copertura il lavoro di giornalista), ecco tutte queste cose che potenzialmente mi basterebbe un clic per farle, mi danno un tale senso di tranquillità nel rapporto con gli altri che mi fermo lì. Cosa dalla quale derivano due benefici in più. Primo: non rischio di infrangere la legge (anche voi non dovrete farlo), evitando così, tra l'altro, che i vari *Porta a Porta*, *Matrix* e compagnia bella mi fracassino le scatole occupandosi di me una sera sì e una no. Secondo: capisco una volta di più come funzionano questi aggeggini elettronici che riempiono le nostre vite con tutta la loro pretesa intelligenza. Perché poi, dietro a ogni magia che Riccardo ci illustra, c'è sempre un meraviglioso errore umano, c'è sempre qualcuno che, nel tentativo di regalare un po' di cervello a un computer o a un telefonino che altrimenti sarebbe un perfetto deficiente, salta un passaggio o dimentica un controllo. E ricorda così a tutti noi che quelle che abbiamo davanti sono solo scatolette, utilissime per carità, ma scatolette. È una certezza che a volte, quando gli apocalittici riescono quasi a convincermi che in futuro saremo tutti schiavi delle macchine, mi fa dormire più tranquillo.

Insomma, finisce che un libro che dovrebbe svelarmi qualcosa sul mondo dell'informatica si trasforma invece in una specie di raccolta di fiabe della buona notte per il mio io inquieto. Dite che sono messo male? Facciamo che, finito di leggere, mi raccontate anche voi che effetto vi fa.

*Federico Bona*

# Introduzione

## Il lato oscuro dell'investigatore...

... non è quello che sta controluce, tanto per capirci.

Uffa, sono partito con la battuta, mentre, per una volta, volevo dare un tono di serietà all'introduzione di un mio libro. Pazienza, resta il fatto che non sei certo qui per ammirare la mia folta chioma di capelli.

Scommetto che vuoi imparare qualcosa sulle investigazioni informatiche. Come sono perspicace, vero? E io, sai che faccio? Rilancio, con un secondo capitolo de *L'investigatore informatico*, che va in direzione opposta, ma complementare, al primo.

Mi spiego. Se guardi ogni tanto la TV, hai di sicuro notato che esistono due tipi di investigatori. Quelli tutti d'un pezzo, ligi al dovere e al codice di comportamento. Insomma, gente che segue le regole al millimetro e guai a chi le sgarra. Pensa a uno qualsiasi dei "capi" di una serie CSI e mi hai capito. E poi? Poi ci sono gli investigatori che, pur facendo del bene, usano dei metodi a volte "discutibili". Per esempio, quando serve alzano le mani o buttano giù una porta senza mandato.

Il primo "*L'investigatore informatico*" ti mostra alcune tecniche e procedure che rientrano nel primo caso, mentre questa seconda puntata rientra nell'altra sfera. E non ti sto dicendo che insegno a lanciare il monitor del tuo computer per spaccare una finestra e intrufolarti nell'appartamento di un sospettato. Più semplicemente, nelle pagine che seguono, trovi moltissimi trucchi "non autorizzati", o top-secret, che svelano come alcuni esperti riescono a penetrare i sistemi di difesa di un computer e magari a prenderne possesso. E, già che ci sono, "prelevare" dati e informazioni altrui.

Che poi questi esperti lo facciano per scopi genuini, oppure perché sono dei truffatori, in realtà, ci importa poco. Perché, se è vero che ti insegno passo dopo passo come replicare queste procedure, è pur vero che lo faccio con un fine sempre e solo didattico, utile per imparare a difenderti da chi ti vuole fregare in Rete.

E così, eccoci all'inizio di un viaggio nato un po' per caso e un po' no. Alla base, il successo smodato del primo *"L'investigatore informatico"*. Davvero, non pensavo che un libro di questo tipo potesse richiamare tanta attenzione e tanti lettori, e ti ringrazio se lo hai scelto per passare qualche ora di sano divertimento informatico. Se non lo hai fatto, sappi che, solo per aver letto queste righe, sei ora obbligato ad acquistare i fascicoli di un'enciclopedia per il resto della tua vita. Dai, scherzo. Anzi, sappi che i due volumi non hanno niente a che fare l'uno con l'altro. Anche se non hai letto il primo, potrai capire il secondo senza problemi e viceversa. Semplicemente, uno tratta il lato buono delle investigazioni, e l'altro (cioè questo), quello più "underground".

## Un libro "suggerito"

Ma torniamo alle origini di queste pagine, dovute, dicevamo, al successo del primo volume e... ai tanti suggerimenti ricevuti da chi l'ha letto. Giuro: tutti ne sono stati entusiasti, ma nell'inviarmi i loro complimenti, hanno colto l'occasione per offrirmi nuovi spunti. E ti pareva, sempre pronti a farmi fare le notti di lavoro!

Così sono venuto a sapere di gente che, grazie al primo *"L'investigatore informatico"*, ha scoperto, con l'analisi di documenti ed e-mail, che la moglie o la fidanzata lo stava tradendo. Altri, con le tecniche e le procedure spiegate, sono riusciti a scovare un temibile "trojan" (se non sai cos'è nei prossimi capitoli lo capirai fin troppo bene) nel proprio computer o qualche programma-spia installato da un concorrente, che stava rubando dati preziosi.

Sono solo alcuni esempi della fantasia con la quale i miei lettori hanno ben pensato di sfruttare quanto gli ho insegnato. Cose che emozionano anche il più duro e navigato degli autori, figuriamoci un tenerone come me. E così, io e la mitica Apogeo, ci siamo chiesti se non fosse stato il caso di elargire informazioni e tecniche ancora più "scottanti", puntando magari a quelle che nessuno ti spiega in modo facile, perché facili non sono.

Il fatto è che la difficoltà del mio lavoro, che considero il più bello del mondo (dai, anche fare l'editore di Playboy USA non deve essere malaccio), sta proprio nel semplificare concetti e nozioni, per farli capire anche a chi non ha il tempo o le competenze per farlo. Ma lo scopo di questo secondo episodio, in realtà, è anche un altro. Vuole infatti spiegare dei concetti sfiziosissimi per i meno esperti, ma utili anche a chi mastica informatica da mattina a sera. Con la premessa, che è poi quella che faccio per tutti i miei libri, che alcune semplificazioni possono fare ribaltare dalla sedia i lettori più navigati, ma sono lì proprio per rendere appetibili a tutti gli argomenti trattati.

Ah già, prima di parlarti proprio degli argomenti, una precisazione importante. Non sai un tubo d'informatica? Riesci a malapena a spostare il mouse? Sei il lettore perfetto per le pagine che seguono. Perché parto dal presupposto che tu non sappia nulla, o quasi, di computer. Anche con una sana dose d'ignoranza informatica, dunque, preparati a un viaggio misterioso, in un mondo di peccati digitali e segreti mai svelati in merito d'investigazioni, truffe e sicurezza informatica.

## **E ora... i capitoli!**

Al primo capitolo, il compito di spiegarti nei dettagli ciò che stai per fare.

Ma passando al lato pratico, hai presente la password che protegge l'accesso ad alcuni computer? Forse non sai che è possibile scoprirla sfruttando un programma speciale, che è il protagonista del secondo capitolo.

E che dire del terzo? Qui ti spiego che il computer è come una casetta con porte e finestre e che esistono tecniche che consentono, a chi desidera farlo, di entrare senza bisogno di bussare.

Per farlo, però, servono alcuni strumenti molto particolari, opportunamente svelati dal quarto capitolo.

Così pagina dopo pagina, litri e litri di caffè dopo, arrivi al quinto capitolo. Potrei dirti che è uno dei miei preferiti, ma poi gli altri si offenderebbero, abbandonando queste pagine e lasciandole vuote, buone solo per accendere il fuoco (gli altri possibili utilizzi non li voglio sapere). Ma è pur vero che parlare di "phishing" dal punto di vista di chi lo fa, o lo deve fare, è dannatamente entusiasmante. In fondo, rimanendo in ambito cinematografico, hai mai notato che le fanciulle più sexy (di solito) stanno coi cattivi?

Mentre fantastichi sulla bella vita di certi criminali, arrivi così al sesto capitolo. E qui capisci che, forse, è meglio stare dalla parte dei buoni. Infatti ti spiego cosa è possibile fare nel caso in cui un cattivo cada nel nostro tranello. C'è da rimanere di stucco, fidati.

Nel Capitolo 7, spazio invece ad alcune tecniche utili per svelare cosa si digita su un computer in tua assenza o ricevere direttamente nel tuo indirizzo di posta elettronica un rapporto con le "attività" svolte su un elaboratore. Roba da fantascienza? Quasi, resta il fatto che te la metto davanti su un piatto d'argento (facciamo d'oro, bando all'avarizia!).

E così eccoti al Capitolo 8. Qui passo e chiudo, regalandoti vere e proprie chicche che si rivolgono ai telefonini e, siediti immediatamente, alla creazione di programmi in grado di prendere il controllo dei computer altrui!

Nelle pagine finali, invece l'elenco delle "porte", vale a dire i punti di accesso, autorizzati o meno che siano, per far visita a qualcuno via Internet.

## **Quattro chiacchiere tra amici**

Insomma, se ti sei fatto l'idea di un libro "tosto", credo non ti stia sbagliando. Di sicuro "tosti" sono i suoi argomenti, mentre lo stile con il quale te li insegno vuole essere, come sempre, diretto, colloquiale e, spero, divertente. Di mio, reputo che, per essere divertenti nello spiegare la tecnologia, ci si debba divertire nel farlo. E ti posso garantire che, in questo libro più che mai, mi sono divertito come un pazzo.

Ti lascio dunque al resto di questo curioso libro, con la speranza che un sorriso si sia già dipinto sulle tue labbra. In caso contrario, ricordati che c'è sempre quell'enciclopedia da pagare. Se devi essere serio, tanto vale che tu lo sia per qualcosa, no?

Buon divertimento e grazie per essere qui!

*Riccardo "Ricky" Meggiato*

P.S. Come al solito, se vuoi contattarmi o scoprire che numero di scarpe porto (dico per dire), visita il mio sito ufficiale, [www.riccardomeggiato.com](http://www.riccardomeggiato.com).