

Le 10 regole dell'hacking

(tratto da *La Stampa* di venerdì 9 luglio 1999: intervista di Salvatore Romangolo a Raoul Chiesa)

Fare hacking - vale a dire introdursi in sistemi informatici attraverso le reti di telecomunicazione - è una pratica che si sta diffondendo sempre di più, complici i mass-media, il cinema, le azioni epiche o meno epiche intraprese da hacker europei e statunitensi.

Come tutte le "arti", però, anche l'hacking ha delle regole fisse le quali - se rispettate - aiutano molto la persona a diventare bravo ed innalzare il proprio livello di capacità (skill).

Suddividerei le "regole" in due aree...le regole da rispettare, ed i consigli per migliorare.

Le "regole d'oro", i comportamenti che distinguono un hacker serio e capace dal ragazzino che gioca e non sa quello che sta facendo, sono le seguenti:

1. mai far danni al sistema che violi, se ciò non è strettamente necessario, e comunque esclusivamente se server ad evitare pericoli a te o ad altri di cui ti importa
2. rispettare, curare ed *ottimizzare* ove possibile, il sistema che violi.
3. mai far danni a singoli individui (privati ed utenze finali)
4. rispettare il lavoro altrui (sistemistico)
5. ove possibile (è difficile....ma ogni tanto e' riuscita come cosa) aiutare il system manager, informandolo e parlandoci; se ciò non è fattibile, salvaguardare la sicurezza di quel sistema informatico.

Queste, quindi, le regole d'oro di *comportamento*. Veniamo ora alle regole di *formazione tecnica*.

6. Apprendere, studiare, imparare quanto più possibile. La Rete è piena di siti con documentazione di qualunque tipo: dal java all'html, passando per Linux e Windows NT, proseguendo per l'analisi e l'elenco dei bug (difetti di programmazione) di ogni sistema operativo esistente al mondo: leggere, leggere ed ancora leggere.
7. Utilizzare l'help del sistema operativo che si viola e ancora non ci conosce. Imparare i comandi, i sottocomandi, i trucchi.
8. Saper programmare...un conto è utilizzare un software scritto da terzi per "hackerare" un sistema, un altro conto è scriversi da soli il programma ed utilizzarlo, facendogli fare quello che ci siamo prefissi
9. Tenersi costantemente aggiornati. L'hacking (dal quale deriva di immediata conseguenza la sicurezza informatica) è in aggiornamento esponenziale: ogni giorno escono almeno una decina di bug, difetti, trucchi, scoperte, patch software....bisogna "girare" per i siti più aggiornati, andare in quelli più conosciuti ed in quelli meno famosi, e vedere cosa c'è di nuovo.
10. Essere umili. Molto spesso l'umiltà aiuta. Essendo umili, troverai con molta più facilità qualcuno disposto ad aiutarti, insegnarti, "aperti gli occhi". Avere cultura. Cultura in campo hacking significa avere un background culturale, sapere cosa c'era in Italia prima di Internet, sapere che ci sono altri tipi di reti, protocolli e sistemi operativi, oltre a quelli più conosciuti.

Riferimenti utili:

Siti:

<http://www.kevinmitnick.com>
sito ufficiale dell'hacker più famoso del mondo, Kevin Mitnick

<http://www.phrack.com>
Phrack Magazine: il magazine elettronico & underground più importante e storico

<http://www.2600.com>

2600 Magazine

<http://www.l0pht.com>
L0pht Heavy Industries

<http://www.cultdeadcow.com/>
The Cult of the Dead Cow: i creatori del Back Orifice per attaccare sistemi Microsoft-based

Libri

Hacker's Crackdown: giro di vite contro gli hackers, ediz. Shake Milano
Spaghetti hacker, ediz. Apogeo
Sulle tracce di Kevin, ediz. Sperling & Kupfler

Tesi di laurea

Il Web Oscuro: origine, sviluppo e percezione dell'hacking in Italia. **Enrico Novari**, anno accademico 1998/99, Università La Sapienza di Roma, Corso di Laurea in Scienza della Comunicazione, Cattedra di Sociologia della Comunicazione, 110 e lode, Relatore Prof. Mario Morcellini.

© Tutto il materiale contenuto in questo file, in qualunque forma espresso, è protetto dalle leggi sul diritto d'autore.