

Ethical Hacking

Nel contesto della sicurezza informatica, con il termine **Hacker** viene indicato un tecnico in grado di individuare delle vulnerabilità o debolezze in un software e di sfruttarle per prendere possesso o trarre vantaggio da un sistema informatico sul quale non sarebbe in grado di poter operare. Come più volte detto, un sistema software molto raramente si può ritenere *perfetto* sia sotto il profilo funzionale sia sotto il profilo della sicurezza.

Un *Hacker* può essere spinto da diverse motivazioni alla ricerca di vulnerabilità nel software, tra cui il desiderio di mostrare la propria abilità o la ricerca di un profitto personale, ma a volte può essere mosso anche dal desiderio di individuare le debolezze di un software per assistere la società che lo ha prodotto nella risoluzione e nella *messa in sicurezza* del programma stesso.

Storicamente si sono quindi individuate diverse *fazioni* di *hacker* che si sono suddivise a seconda dei propositi. La distinzione più marcata è quella che distingue i cosiddetti *White hat* (letteralmente *cappelli bianchi*) dai *Black hat* (letteralmente *cappelli neri*), attribuendo ai primi un comportamento *non maligno* e quindi più etico rispetto ai secondi.

È così stato coniato il termine di *Ethical Hacking* (letteralmente *Hacking etico*) con il quale si definiscono le attività degli esperti informatici che si occupano di sicurezza e svolgono il loro lavoro ricercando vulnerabilità e difetti nei sistemi informatici con diversi scopi etici:

- La condivisione delle informazioni scoperte;
- Libero accesso alle informazioni per tutti;
- Miglioramento della vita di tutti nel mondo.

Lo stesso movimento del software libero e a sorgente aperto, il cosiddetto *free software movement* il quale ha dato corso allo sviluppo del *free and open source software*, ha tratto le sue origini dal movimento dei *White hat hackers*.

Ancora oggi esiste una diffusa controversia nell'interpretazione del termine *hacker* che in taluni contesti ha ancora un'accezione che accomuna il termine al criminale informatico. Tuttavia esistono anche percorsi di formazione e di certificazione delle competenze nel campo della sicurezza, che per esempio l'*EC-Council* (sito web <http://www.eccouncil.org/>), un'organizzazione di professionisti della sicurezza informatica, certifica con il percorso formativo il *CEH: Certified Ethical Hacker*, un professionista che capisce e conosce il modo di cercare le vulnerabilità e le debolezze nei sistemi e utilizza gli stessi strumenti e le stesse conoscenze dei soggetti malintenzionati, ma in maniera legale e al solo scopo di migliorare la sicurezza di sistemi e utenti.