Prefazione

Viviamo in un'epoca in cui gli hacker hanno una grande influenza. L'hacking, oggi, può avere un impatto sulla vita di milioni di persone, prendendo di mira elezioni, reti elettriche e tutte le infrastrutture su cui le persone fanno affidamento per le loro attività quotidiane, per non parlare del loro benessere.
Nel 2021, gli hacker hanno utilizzato un ransomware (un "attacco a riscatto") per chiudere il più grande gasdotto degli Stati Uniti. Ciò ha causato preoccupazioni, cancellazioni di voli e carenze. L'attacco, ben eseguito, ha avuto carattere personale per coloro che ne hanno sperimentato in prima persona l'impatto.
Dato il loro livello di influenza, è imperativo non solo insegnare un hacking etico, ma anche incoraggiarlo. *Ethical Hacking* è un ottimo manuale per quei programmatori che vogliono apprendere i fondamenti della progettazione degli strumenti di hacking, imparando anche a implementare le tecniche utilizzate dai penetration tester professionisti. Per riuscire in questo suo scopo, il libro vi guida attraverso la configurazione di un laboratorio, con molti esercizi che vi forniranno le competenze di cui avrete bisogno.
Occupandosi di hacking su piccola scala, che potrebbero verificarsi in un negozio locale, fino agli hacking su larga scala, a livello aziendale, il libro spazia in modo sorprendente risultando quindi anche un testo ideale per un corso di sicurezza a livello universitario o post-universitario. Considero le lezioni di questo libro necessarie per tutti i professionisti nei campi della tecnologia, della politica e della leadership, attuali e futuri.
Nel bene e nel male, l'hacking è qui per restare.

Juan Gilbert
Andrew Banks Family Preeminence Endowed Professor
e Chair Herbert Wertheim College of Engineering
University of Florida