

Prefazione

Ogni anno partecipo a varie conferenze sulla sicurezza in tutto il mondo. Un oratore che non mi sono mai perso è Johnny Long. Non è solo il fatto che Johnny è uno degli oratori più brillanti nell'ambito della sicurezza: le sue presentazioni sono ricche di idee interessanti che si basano sulla vera e propria pietra miliare che dovrebbe essere la prima linea di difesa nel campo della sicurezza: il buonsenso.

Non solo Johnny ti invita a non ignorare le cose più ovvie e a essere più attento a ciò che ti circonda; il suo approccio non tecnologico all'hacking gli consente di aggirare le più costose e sofisticate tecnologie di sicurezza, che talvolta rappresentano l'unica forma di difesa di dati e beni.

Ogni giorno, le aziende spendono migliaia di dollari in difese di sicurezza ad alta tecnologia, ma sottovalutano le semplici tecniche che gli hacker non tecnologici possono sfruttare a proprio vantaggio. In questo libro, Johnny presenta tante tecniche da condurre alla luce del sole e che tutti i professionisti della sicurezza dovrebbero tenere in considerazione. Nella fretta di portare a termine i propri compiti e di passare all'impegno successivo, molti responsabili della sicurezza sottovalutano le tecniche più semplici, in grado di aver ragione anche delle tecnologie di sicurezza più costose.

Proprio questo vizio dei dipartimenti di sicurezza, che tendono a ignorare le minacce semplici, favorisce gli attacchi. Un intruso escogiterà l'attacco in cui pensa di trovare la minore resistenza, mentre molte aziende si preparano a rispondere ad attacchi da Mission Impossible. Johnny vi sorprenderà aggirando una sicurezza fisica con uno straccio, sfruttando un gruppo di impiegati per entrare in un edificio, immergendosi nei cassonetti alla ricerca di informazioni riservate, utilizzando Google e le reti P2P per individuare informazioni riservate pubblicate da dipendenti e utenti e poi spiegando come sia possibile mettere insieme tutte queste cose per preparare un attacco.

L'elemento più sottovalutato nella sicurezza di un'attività è il fattore umano. Le tecnologie più costose non offrono alcun vantaggio se chiunque può chiamare un impiegato e convincerlo a disattivare il sistema di sicurezza o ad alterare le sue impostazioni per creare una finestra di opportunità. L'ingegneria sociale è l'arma preferita di molti hacker. Perché sprecare tempo su elaborate strategie tecniche, quando basta fare una chiamata per acquisire informazioni apparentemente innocue da persone assolutamente ignare e sfruttarle per aprire la porta?

Nella mia vita passata di hacker black-hat, l'ingegneria sociale mi ha consentito di aprire una porta in tempi record, pochi minuti. Poi, per conseguire i miei obiettivi, ho dovuto impiegare attacchi più tecnici. L'esempio di ingegneria sociale che Jack Wiles fornisce in questo libro può sembrare fin troppo bello per essere vero. Ebbene non lo è affatto. E questa non è che una delle tante idee: l'immaginazione umana può crearne molte, molte altre. La domanda è: voi, i vostri colleghi, i vostri dipendenti o i vostri genitori ci cascheranno? Il capitolo sull'ingegneria sociale descrive magistralmente il modo in cui gli hacker non tecnologici manipolano le loro vittime con quello che, probabilmente, è il metodo di attacco più comune, contro il quale non c'è soluzione tecnologica che tenga.

Sia i normali utenti, sia le aziende troveranno in queste pagine informazioni preziose per aumentare la propria consapevolezza. Questo libro illustra chiaramente le minacce, spesso ignorate, che i manager informatici devono tenere in considerazione quando sviluppano i piani di sicurezza per proteggere la propria azienda. I responsabili di attività commerciali troveranno i contenuti di questo libro parecchio interessanti; i consumatori acquisiranno conoscenze sui metodi utili per proteggere se stessi dai ladri di identità, dai furti e per perfezionare le difese dei sistemi domestici gestiti da un computer.

Come nel suo *Google Hacking*, Johnny offre, ancora una volta, una divertente e illuminante panoramica sulle tecniche di hacking e su come l'ingenuità possa essere sfruttata dai vostri avversari.

Kevin Mitnick