Introduzione

"Alzarsi e rialzarsi ancora, finché gli agnelli diventeranno leoni"

Questa citazione dal film *Robin Hood* di Russell Crowe (2010) è più che mai adatta alla settima edizione di questo libro. Non fraintendete: oggi siamo gli agnelli, mandati al macello ogni minuto del giorno. Ma *non può* continuare. *Non possiamo* permetterlo. Le conseguenze sono troppo gravi. Catastrofiche.
Vi imploriamo di leggere ogni parola di ogni pagina e prendere sul serio questo avvertimento. *Dobbiamo* capire come lavorano i malintenzionati e utilizzare le contromisure descritte in queste pagine (e altre ancora), oppure continueremo a essere macellati e il nostro futuro sarà compromesso.

Argomenti del libro

Abbiamo rielaborato l'intero contenuto del libro, ma desideriamo evidenziare in particolare alcuni temi nuovi di fondamentale importanza. Nel libro abbiamo introdotto un tema sempre più al centro dell'attenzione, quello delle minacce avanzate persistenti, o APT (*Advanced Persistent Threats*), fornendo esempi tratti dal mondo reale di come questi attacchi abbiano avuto successo e mostrando come rilevarli e bloccarli. Abbiamo poi aggiunto una parte nuova dedicata al mondo dell'hacking embedded, trattando le tecniche usate dagli hacker per rimuovere da una scheda tutti i suoi chip, effettuare il reverse engineering e scoprire il tallone di Achille nel complesso mondo di 1 e 0. Un'altra parte nuova tratta l'hacking di database, esaminando i bersagli e le tecniche usate per sottrarre dati sensibili. Un intero capitolo è dedicato al mondo mobile, descrive il mondo embedded di tablet, smartphone e dispositivi vari, e mostra come gli hacker stiano concentrandosi su questa nuova area d'attacco esplosa negli ultimi anni. E infine, come avremmo dovuto fare fin dalla primissima edizione del 1999, abbiamo aggiunto un intero capitolo dedicato alle contromisure, dove assumiamo un ruolo attivo nello spiegare ciò che voi, amministratori o utenti finali, potete fare per evitare che gli hacker entrino nei vostri sistemi.

Come usare questo libro

Lo scopo di questo libro è presentare il mondo degli hacker: come ragionano e come lavorano. Ma è altrettanto importante spiegare i modi per fermarli. Usate questo libro come riferimento per entrambi questi scopi.

Struttura del libro

Nella prima parte esaminiamo i modi in cui gli hacker acquisiscono informazioni sui loro bersagli. Spesso procedono in modo meticoloso per capire i loro obiettivi d'attacco ed enumerarne tutti i dettagli, e nel testo mostriamo le basi delle loro tecniche. Nella seconda

parte esponiamo l'obiettivo ultimo di qualsiasi hacker: arrivare al desktop o al server, con un nuovo capitolo dedicato alle minacce avanzate persistenti o APT. La terza parte esamina i modi con cui gli hacker attaccano le autostrade dell'informazione a cui i nostri sistemi si connetto. Questa parte include nuovi materiali dedicati all'hacking di sistemi embedded. La quarta parte esamina il mondo del Web e dei database, oltre alle opportunità di hacking nel mondo mobile, e presenta anche le contromisure che si possono utilizzare.

Convenzioni

Anche in questa edizione abbiamo mantenuto la struttura delle precedenti; ogni tecnica di attacco è evidenziata da un'icona come quelle riportate di seguito.

Icona dell'attacco

Facilita l'individuazione di specifici strumenti e metodologie di hacking. A ogni attacco corrisponde una contromisura con suggerimenti pratici, specifici, testati sul campo, indicati da un'icona speciale.

Icona della contromisura

Passate subito alla soluzione dei problemi e lasciate indietro gli hacker.

- Prestate attenzione alle parti evidenziate in grassetto nei listati di codice, che indicano l'input dell'utente.
- Ogni attacco è accompagnato da un grado di rischio ricavato da tre componenti valutati in base all'esperienza degli autori.

Popolarità:	la frequenza di utilizzo verso bersagli attivi; 1 indica la frequenza minima, 10 la massima.
Semplicità:	il livello di conoscenze e capacità necessario per eseguire l'attacco; 1 indica un programmatore esperto nella sicurezza, 10 un principiante.
Impatto:	il potenziale danno causato dall'esecuzione dell'attacco, in caso di successo; 1 indica la scoperta di informazioni banali sul bersaglio, 10 la compromissione dell'account del superuser o equivalente.
Grado di rischio:	il grado di rischio complessivo (media dei tre valori precedenti).

Ringraziamenti

Gli autori ringraziano gli editor e lo staff di produzione di McGraw-Hill Professional che ha lavorato su questa settima edizione, tra cui Amy Jollymore, Ryan Willard e LeeAnn Pickrell; senza il loro impegno non sarebbe stato possibile realizzare il prodotto che avete nelle vostre mani. Siamo davvero grati per aver potuto lavorare con un team così agguerrito che ci ha aiutato nel nostro impegno a spiegare come ragionano e lavorano gli hacker.
Un ringraziamento speciale a tutti i collaboratori e i revisori tecnici di questa edizione, e un enorme "Grazie" a tutti i nostri devoti lettori. Avete fatto di questo libro un grande successo mondiale. Non potremo mai ringraziarvi abbastanza!