

Indice dell'opera

Volume 1

Prefazione	v
Introduzione	ix
Capitolo 1 – L'idea di hacking	1
Capitolo 2 – Programmazione	7
0x210 Che cos'è la programmazione?	8
0x220 Pseudocodice	10
0x230 Strutture di controllo	10
0x240 Altri concetti fondamentali di programmazione.....	15
0x250 Iniziamo a sporcarci le mani.....	24
0x260 Torniamo alle basi	47
0x270 Segmentazione della memoria.....	87
0x280 Costruire sulle fondamenta	104
Capitolo 3 – Exploit.....	149
0x310 Tecniche di exploit generalizzate	153
0x320 Buffer overflow.....	153
0x330 Esperimenti con la shell BASH	172
0x340 Overflow in altri segmenti	193
0x350 Stringhe di formato	219
Capitolo 4 – Strutture di rete	253
0x410 Il modello OSI	253
0x420 Socket	256
0x430 I livelli inferiori	281
0x440 Sniffing di rete	290
Riferimenti	327

Volume 2**Prefazionev****Introduzioneix****Capitolo 1 – Attacchi di rete 1**

0x110 DoS (Denial of Service) 1

0x120 Dirottamento TCP/IP 10

0x130 Scansione di porte 18

0x140 Qualche hack in pratica 30

Capitolo 2 – Shellcode43

0x210 Assembly e C 43

0x220 Il percorso dello shellcode 50

0x230 Shellcode che avvia una shell 62

0x240 Shellcode per il binding di porte 72

0x250 Shellcode di connect-back 87

Capitolo 3 – Contromisure95

0x310 Contromisure che rilevano gli attacchi 96

0x320 Daemon di sistema 97

0x330 Strumenti del mestiere 108

0x340 File di log 115

0x350 Trascurare l'ovvio 118

0x360 Camuffamento avanzato 133

0x370 L'infrastruttura completa 142

0x380 Contrabbando del payload 148

0x390 Restrizioni per i buffer 154

0x3a0 Rafforzare le contromisure 171

0x3b0 Stack non eseguibile 171

0x3c0 Spazio nello stack a generazione casuale 175

Capitolo 4 – Crittologia193

0x410 Teoria dell'informazione 194

0x420 Tempo di esecuzione di un algoritmo 197

0x430 Cifratura simmetrica 200

0x440 Cifratura asimmetrica 202

0x450 Sistemi di cifratura ibridi 209

0x460 Cracking delle password 225

0x470 Cifratura su reti wireless 802.11b 247

0x480 Attacchi WEP 251

Riferimenti269

Prefazione



Questo libro è uno dei due volumi realizzati a partire dal testo di Jon Erickson Hacking - The Art of Exploitation (2nd Edition) pubblicato in lingua inglese dall'editore No Starch Press ed edito la prima volta in Italia da Apogeo nel mese di febbraio 2008 con il titolo L'arte dell'hacking - seconda edizione. Il testo originale contava 456 pagine nel formato della collana Guida completa (17 x 24 cm). L'arte dell'hacking volume 1 e 2 ripropongono il testo completo, senza tagli o modifiche. Gli unici cambiamenti sono stati fatti da un punto di vista tipografico, per adattare il contenuto al taglio tascabile della collana Pocket.

Capire le tecniche di hacking è spesso complesso, perché richiede conoscenze ampie e approfondite. Molti testi dedicati all'hacking sono oscuri e confusi proprio perché ci sono delle lacune nella formazione di base. In questo libro si rende più accessibile il mondo dell'hacking presentando il quadro completo delle competenze necessarie: dalla programmazione al codice macchina e alla realizzazione di exploit.

Inoltre il codice sorgente riportato nel libro è scaricabile gratuitamente all'indirizzo <http://www.nostarch.com/download/booksrc.zip>: un utile supporto per la realizzazione di exploit per seguire meglio gli esempi presentati nel testo e fare delle prove pratiche lungo il percorso.

Piano dell'opera

Volume 1

Capitolo 1 – L'idea di hacking

Gli hacker, programmatori creativi: chiarimenti sul nome e sulle origini dell'hacking.

Capitolo 2 – Programmazione

Fondamenti della programmazione in C; scrittura delle prime righe di codice; analisi del codice sorgente di tre semplici giochi d'azzardo per imparare a gestire casualità e permessi multiutente.

Capitolo 3 – Exploit

Gli exploit, ovvero come sfruttare una falla di un programma: tecniche generalizzate; buffer overflow; esperimenti con la shell BASH, overflow in altri segmenti, stringhe di formato.

Capitolo 4 – Strutture di rete

Introduzione alle strutture di rete: il modello OSI, i socket e lo sniffing di dati.

Volume 2

Capitolo 1 – Attacchi di rete

Gli attacchi DoS, dirottamenti TCP/IP, scansione di porte e alcuni esempi su come sfruttare le vulnerabilità dei programmi di rete.

Capitolo 2 – Shellcode

Sfruttare lo shellcode per avere un controllo assoluto sul programma attaccato e ampliare così le potenzialità degli exploit, oltre a sviluppare capacità con l'uso del linguaggio assembly.

Capitolo 3 – Contromisure

Come difendersi (cercare di individuare gli attacchi e difendere la vulnerabilità grazie all'azione dei daemon e all'analisi dei file di log) e come aggirare le difese (creare exploit che non lascino tracce).

Capitolo 4 – Crittologia

Come comunicare in segreto tramite messaggi cifrati e come decifrare tali comunicazioni: crittografia e crittoanalisi.

Ringraziamenti

Desidero ringraziare Bill Pollock e tutto lo staff di No Starch Press per aver reso possibile la realizzazione di questo libro e per avermi consentito di applicare un alto grado di controllo creativo nel processo di produzione. Voglio inoltre ringraziare i miei amici Seth Benson e Aaron Adams per la rilettura e la correzione delle bozze, Jack Matheson per l'aiuto nell'organizzazione dei contenuti, il dott. Seidel per aver mantenuto sempre vivo in me l'interesse per l'informatica, i miei genitori per avermi acquistato il primo Commodore VIC-20 e la comunità degli hacker per lo spirito di innovazione e la creatività che hanno prodotto le tecniche descritte in questo libro.

Introduzione



Nell'edizione originale il testo che segue era parte della conclusione. In questa edizione, ritenendo le idee proposte utili a chi si avvicina alle tematiche affrontate, si è deciso di utilizzarlo per introdurre entrambi i volumi.

L'hacking è un argomento spesso frainteso, e i media amano enfatizzarne gli aspetti, il che peggiora le cose. I tentativi di cambiare la terminologia non hanno portato ad alcunché: occorre cambiare la mentalità. Gli hacker sono semplicemente persone con spirito di innovazione e conoscenza approfondita della tecnologia. Non sono necessariamente criminali, anche se, poiché il crimine talvolta rende, ci saranno sempre dei criminali anche tra gli hacker. Non c'è nulla di male nella conoscenza in dote a un hacker, nonostante le sue potenziali applicazioni.

Che piaccia o meno, esistono delle vulnerabilità in software e reti da cui dipende il funzionamento dell'intero sistema mondiale. È semplicemente un risultato inevitabile dell'eccezionale velocità di sviluppo del software. Spesso il software nuovo riscuote successo anche se presenta delle vulnerabilità. Il successo significa denaro, e questo attrae criminali che imparano a sfruttare tali vulnerabilità per ottenere proventi finanziari. Sembrerebbe una spirale senza fine, ma fortunatamente non tutte le persone che trovano le vulnerabilità nel software sono criminali che pensano solo al profitto. Si tratta per lo più di hacker, ognuno spinto dalle proprie motivazioni; per alcuni è la curiosità, per altri ancora è il piacere della sfida, altri sono pagati per farlo e parecchi sono, in effetti, criminali. Tuttavia la maggior parte di queste persone non hanno intenti malevoli, ma anzi, spesso aiutano i produttori a correggere i loro software. Senza gli hacker, le vulnerabilità e gli errori presenti nel software rimarrebbero occulti.

Sfortunatamente il sistema legislativo è lento e piuttosto ignorante riguardo la tecnologia. Spesso vengono promulgate leggi draconiane e sono comminate

sentenze eccessive per spaventare le persone. Questa è una tattica infantile: il tentativo di scoraggiare gli hacker dall'esplorare e cercare vulnerabilità non porterà a nulla. Convincere tutti che il re indossa nuovi abiti non cambia la realtà che il re è nudo. Le vulnerabilità nascoste rimangono lì dove si trovano, in attesa che una persona più malevola di un hacker normale le scopra.

Il pericolo delle vulnerabilità presenti nel software è che possono essere sfruttate per qualunque fine. I worm diffusi su Internet sono relativamente benigni, rispetto ai tanto temuti scenari terroristici. Tentare di limitare gli hacker con la legge può aumentare le probabilità che si avverino i peggiori scenari, perché si lasciano più vulnerabilità a disposizione di chi non ha rispetto per la legge e vuole davvero causare danni.

Alcuni potrebbero sostenere che se non esistessero gli hacker non vi sarebbe motivo di porre rimedio alle vulnerabilità occulte. È un punto di vista, ma personalmente preferisco il progresso alla stagnazione. Gli hacker giocano un ruolo molto importante nella coevoluzione della tecnologia. Senza di essi non vi sarebbe grande impulso al miglioramento della sicurezza informatica. Inoltre, finché saranno poste domande sul "perché" e il "come", gli hacker esisteranno sempre. Un mondo senza hacker sarebbe un mondo privo di curiosità e spirito di innovazione.

L'intento di questo libro è quello di spiegare alcune tecniche di base per hacking e forse anche di dare un'idea dello spirito che lo pervade. La tecnologia è sempre in mutamento ed espansione, perciò ci saranno sempre nuovi hack. Ci saranno sempre nuove vulnerabilità nel software, ambiguità nelle specifiche di protocollo e una miriade di altri problemi.

Le conoscenze fornite in questo libro sono soltanto un punto di partenza. Spetta a voi ampliarle continuando a riflettere sul funzionamento delle cose, sulle possibilità esistenti e pensando ad aspetti di cui gli sviluppatori software non hanno tenuto conto. Spetta a voi trarre il meglio da queste scoperte e applicare le nuove conoscenze nel modo che riterrete più opportuno.

L'informazione in sé non è un crimine.