1. Record Nr. UNINA9910779875903321

Autore	Mohammed Mohssen <1982, >
Titolo	Automatic defense against zero-day polymorphic worms in communication networks / / Mohssen Mohammed, Al-Sakib Khan Pathan
Pubbl/distr/stampa	Boca Raton, Fla. : , : CRC Press, , 2013
ISBN	0-429-09814-6 1-4822-1905-0 1-4665-5728-1
Descrizione fisica	1 online resource (317 p.)
Collana	Information security books
Classificazione	COM037000COM051230COM053000
Altri autori (Persone)	PathanAl-Sakib Khan
Disciplina	005.8
Soggetti	Computer viruses Computer algorithms Computer networks - Security measures Machine theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	An Auerbach book.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	ch. 1. The fundamental concepts -- ch. 2. Computer networking -- ch. 3. Intrusion detection and prevention systems (IDPSs) -- ch. 4. Honeypots -- ch. 5. Internet worms -- ch. 6. Reading resources on automated signature generation systems -- ch. 7. Signature generation algorithms for polymorphic worms -- ch. 8. Zero-day polymorphic worm collection method -- ch. 9. Developed signature generation algorithms.
Sommario/riassunto	Polymorphic worm attacks are considered one of the top threats to Internet security. They can be used to delay networks, steal information, delete information, and launch flooding attacks against servers. This book supplies unprecedented coverage of how to generate automated signatures for unknown polymorphic worms. Describing attack detection approaches and automated signature generation systems, the book details the design of double-honeynet systems and the experimental investigation of double-honeynet systems. It also discusses experimental implementation of signature-generation algorithms. --

A computer worm is a kind of malicious program that self-replicates automatically and quickly to compromise the security of a computer network. A polymorphic worm is able to change its payload in every infection attempt thereby forcing constant changes to ward off the attacks. Whenever a novel worm is detected in the Internet, the common approach is that the experts from security community analyze the worm code manually and produce a signature. The alternative approach is to find a way to automatically generate signatures that are relatively faster to generate and are of acceptable good quality. This book focuses on how we can automatically generate signatures for unknown polymorphic worms--