Hacking Exposed: Malware and Rootkits

Hacking Exposed: Malware and Rootkits is a useful reference book that gives a unique insight into the techniques behind malware and rootkits. It is a must-read for those responsible for security and a useful addition to the business library.

Malware, rootkits and online attacks are a growing menace faced by everyone who goes online. Going by their proliferation in terms of numbers, reach, intensity and severity, these attacks are on their way to becoming a significant threat to the IT resources of businesses, individuals and nations across the world.

Given the easy availability of online tools and resources to infiltrate and hijack systems, it is important for everyone—especially information security professionals, information systems auditors and those in charge of IT governance—to understand these threats and the damage that they can cause and to learn the countermeasures and defenses available against them.

Hacking Exposed: Malware and Rootkits is a very good resource that focuses on malicious threats such as embedded code, pop-ups, keylogging, rootkits, zombies and bots. It gives detailed information on the latest intrusion detection, firewall, honeynet, antivirus, anticrookit and antispyware technologies.

The book is well written and provides a holistic perspective of the threats, issues and solutions. It also has rich references and resources for readers to learn more about areas of interest or for when situations demand more information.

Positive features of the book include helpful case studies and summaries of countermeasures for each kind of threat. These features are useful to the student, academic and practitioner.

The target audience is information security professionals, system administrators and computer users. It is a valuable resource for the knowledgeable user and for the novice. A good reference for information security managers, security analysts, systems developers, auditors and consultants, it provides useful details in sufficient depth.

Hacking Exposed: Malware and Rootkits is not industry-specific and addresses all sectors of business, industry and public/government sectors, as computer incidents involving malware and rootkits affect all sections in all organizations.

The book is composed of three parts. Part I has two chapters that cover malware methods of infection and malware functionality. Part II consists of four chapters and covers rootkits—user mode, kernel mode, virtual rootkits and the future of rootkits. Part III has five chapters that deal with prevention technologies—antivirus, host protection systems, host-based intrusion prevention, rootkit detection and general security practices. The material is well organized in these three sections with appropriate figures, tables, notes and charts. The appendix provides system integrity analysis, and, while the security methodologies are not cross-referenced, a useful index is provided.

The presentation of Hacking Exposed: Malware and Rootkits is such that it will be of use to the novice, student and seasoned practitioner, and, therefore, it is a recommended good read for those interested in information security.

EDITOR’S NOTE
Hacking Exposed: Malware and Rootkits is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.