1.

Record Nr.	UNINA9910711180503321
Autore	Polk W. Timothy
Titolo	Automated tools for testing computer system vulnerability / / W. Timothy Polk
Pubbl/distr/stampa	Gaithersburg, MD : , : U.S. Dept. of Commerce, National Institute of Standards and Technology, , 1992
Descrizione fisica	1 online resource
Collana	NIST special publication ; ; 800-6
Altri autori (Persone)	PolkW. Timothy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	1992. Contributed record: Metadata reviewed, not verified. Some fields updated by batch processes. Title from PDF title page. Withdrawn.
Nota di bibliografia	Includes bibliographical references.
Sommario/riassunto	Computer security "incidents" occur with alarming frequency. The incidents range from direct attacks by both hackers and insiders to automated attacks such as network worms. Weak system controls are frequently cited as the cause, but many of these incidents are the result of improper use of existing control mechanisms. For example, improper access control specifications for key system files could open the entire system to unauthorized access. Moreover, many computer systems are delivered with default settings that, if left unchanged, leave the system exposed. This document discusses automated tools for testing computer system vulnerability. By analyzing factors affecting the security of a computer system, a system manager can identify common vulnerabilities stemming from administrative errors. Using automated tools, this process may examine the content and protections of hundreds of files on a multi-user system and identify subtle vulnerabilities. By acting on this information, system administrators can significantly reduce their systems' security exposure. This document examines basic requirements for vulnerability testing tools and describes the different functional classes of tools. Finally, the

document offers general recommendations about the selection and distribution of such tools.