1. Record Nr. UNISALENTO991003250019707536

Titolo	Penetration tester's open source toolkit. [electronic resource] / Johnny Long ... [et al.] ; foreword by Max Moser
Pubbl/distr/stampa	Rockland, MA : Syngress Publishing., 2006.
ISBN	9781597490214 1597490210
Descrizione fisica	xxix, 704 p. : ill. ; 23 cm. + 1 CD-ROM (4 3/4 in.)
Altri autori (Persone)	Long, Johnny.author
Disciplina	005.8
Soggetti	Computer security Computer networks - Security measures Electronic books.
Lingua di pubblicazione	Inglese
Formato	Risorsa elettronica
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Chapter 1. Know Your Target. Verify that the IP range or domain belongs to the correct target, perform basic reconnaissance and identify possible target user accounts. Chapter 2. Host Detection Chapter 3. Service Detection Chapter 4. Use port scan tool to enumerate open ports Chapter 5. Using "nmap" to perform a portscan Chapter 6. Using "scanrand" to perform a portscan Chapter 7. Results: List of open ports Chapter 8. Application Fingerprinting Chapter 9. Password Attacks Chapter 10. Exploiting Identified Vulnerabilities Chapter 11. Use exploit toolkits Chapter 12. Using "metasploit framework" to verify and exploit vulnerabilities. Chapter 13. "CGE" to exploit vulnerabilities in Cisco devices.
Sommario/riassunto	Penetration testing a network requires a delicate balance of art and science. A penetration tester must be creative enough to think outside of the box to determine the best attack vector into his own network, and also be expert in using the literally hundreds of tools required to execute the plan. This book provides both the art and the science. The authors of the book are expert penetration testers who have developed many of the leading pen testing tools; such as the Metasploit framework. The authors allow the reader inside their heads to unravel the mysteries of thins like identifying targets, enumerating hosts,

application fingerprinting, cracking passwords, and attacking exposed vulnerabilities. Along the way, the authors provide an invaluable reference to the hundreds of tools included on the bootable-Linux CD for penetration testing. * Covers both the methodology of penetration testing and all of the tools used by malicious hackers and penetration testers * The book is authored by many of the tool developers themselves * This is the only book that comes packaged with the "Auditor Security Collection"; a bootable Linux CD with over 300 of the most popular open source penetration testing tools.