1.

Record Nr.	UNINA9910791006503321
Autore	Buchanan Cameron
Titolo	Kali Linux CTF Blueprints : build, test, and customize your own Capture the Flag challenges across multiple platforms designed to be attacked with Kali Linux / / Cameron Buchanan
Pubbl/distr/stampa	Birmingham, England : , : [Packt] Publishing, , 2014 ©2014
ISBN	1-78398-599-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (190 p.)
Collana	Community Experience Distilled
Disciplina	005.8
Soggetti	Computer security Computers - Access control Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Sommario/riassunto	Build, test, and customize your own Capture the Flag challenges across multiple platforms designed to be attacked with Kali Linux In Detail As attackers develop more effective and complex ways to compromise computerized systems, penetration testing skills and tools are in high demand. A tester must have varied skills to combat these threats or fall behind. This book provides practical and customizable guides to set up a variety of exciting challenge projects that can then be tested with Kali Linux. Learn how to create, customize, and exploit penetration testing scenarios and assault courses. Start by building flawed fortresses for Windows and Linux servers, allowing your testers to exploit common and not-so-common vulnerabilities to break down the gates and storm the walls. Mimic the human element with practical examples of social engineering projects. Facilitate vulnerable wireless and mobile installations and cryptographic weaknesses, and replicate the Heartbleed vulnerability. Finally, combine your skills and work to create a full red-team assessment environment that mimics the sort of corporate network encountered in the field. What You Will Learn Set up

vulnerable services for both Windows and Linux Create dummy accounts for social engineering manipulation Set up Heartbleed replication for vulnerable SSL servers Develop full-size labs to challenge current and potential testers Construct scenarios that can be applied to Capture the Flag style challenges Add physical components to your scenarios and fire USB missile launchers at your opponents Challenge your own projects with a best-practice exploit guide to each scenario