1. Record Nr. UNINA9910786551403321

Autore	Makan Keith
Titolo	Penetration testing with the Bash shell : make the most of the Bash shell and Kali Linux's command-line-based security assessment tools / / Keith Makan
Pubbl/distr/stampa	Birmingham, England : , : Packt Publishing Ltd, , 2014 ©2014
ISBN	1-84969-511-3
Edizione	[1st edition]
Descrizione fisica	1 online resource (151 p.)
Collana	Community Experience Distilled
Disciplina	005.8092
Soggetti	Penetration testing (Computer security) - Examinations User interfaces (Computer systems) - Design
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; Disclaimer; About the Author; About the Reviewers; www.PacktPub.com; Preface; Chapter 1: Getting to Know Bash; Getting help from the man pages; Navigating and searching the filesystem; Navigating directories; Listing directory contents; Searching the filesystem; Directory traversal options; File testing options; File action options; Using I/O redirection; Redirecting output; Redirecting input; Using pipes; Getting to know grep; Regular expression language - a crash course; Regular expression matcher selection options; Regular expression matching control options Output control optionsFile selection options; Summary; Further reading; Chapter 2: Customizing Your Shell; Formatting the terminal output; The prompt string; Prompt string customizations; Aliases; Customizing the command history; Protecting sensitive information from leakage; Customizing tab completion; Summary; Further reading; Chapter 3: Network Reconnaissance; Interrogating the Whois servers; Interrogating the DNS servers; Using Dig; Using dnsmap; Enumerating targets on the local network; Host discovery with Arping; Target enumeration with Nmap; Summary; Further reading Chapter 4: Exploitation and Reverse EngineeringUsing the Metasploit command-line interface; Getting started with msfcli; Using invocation modes with msfcli; Bash hacks and msfcli; Preparing payloads with

Metasploit; Creating and deploying a payload; Disassembling binaries; Disassembling with Objdump; A note about the reverse engineering assembler code; Debugging binaries for dynamic analysis; Getting started with GDB; Setting execution breakpoints and watch points; Inspecting registers, memory values, and runtime information; Summary; Further reading
Chapter 5: Network Exploitation and MonitoringMAC and ARP abuse; Spoofing MAC addresses; Abusing address resolution; Man-in-the-middle attacks; Ettercap DNS spoofing; Interrogating servers; SNMP interrogation; SMTP server interrogation; Brute-forcing authentication; Using Medusa; Traffic filtering with TCPDump; Getting started with TCPDump; Using the TCPDump packet filter; Assessing SSL implementation security; Using SSLyze; Bash hacks and SSLyze; Automated web application security assessment; Scanning with SkipFish; Scanning with Arachni; Summary; Further reading; Index

Sommario/riassunto

An easy-to-understand, step-by-step practical guide that shows you how to use the Linux Bash terminal tools to solve information security problems. If you are a penetration tester, system administrator, or developer who would like an enriching and practical introduction to the Bash shell and Kali Linux command-line-based tools, this is the book for you.