1. Record Nr. UNISA996384743303316

Autore	Harflete Henry <fl. 1653.>
Titolo	Ouranodeisis, cœlorum declaratio [[electronic resource]] : an ephemeris for the yeer of Christ, 1656 ... calculated for the meridians of the two ancient port towns of Sandwich and Dover ... / / by Henry Harflete
Pubbl/distr/stampa	London, : Printed by T.R. and E.M. for the Company of Stationers, 1656
Descrizione fisica	[31], 16 p. : ill
Soggetti	Almanacs, English Ephemerides Astrology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	First word of title in Greek characters. Reproduction of original in the Bodleian Library.
Sommario/riassunto	eebo-0014

2. Record Nr. UNINA9910814080603321

Autore	Cardwell Kevin
Titolo	Building virtual pentesting labs for advanced penetration testing : build intricate virtual architecture to practice any penetration testing technique virtually / / Kevin Cardwell ; cover image by Tony Shi
Pubbl/distr/stampa	Birmingham, [England] : , : Packt Publishing, , 2014 ©2014
ISBN	1-78328-478-1
Descrizione fisica	1 online resource (430 p.)
Collana	Community Experience Distilled
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security - Testing Computers - Access control
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Introducing Penetration Testing; Security testing; Authentication; Authorization; Confidentiality; Integrity; Availability; Non-repudiation; Abstract testing methodology; Planning; Nonintrusive target search; Intrusive target search; Data analysis; Reporting; Myths and misconceptions of pen testing; Summary; Chapter 2: Choosing the Virtual Environment; Open source and free environments; VMware Player; VirtualBox; Xen; Hyper-V; vSphere Hypervisor; Commercial environments vSphereVMware Player Plus; XenServer; VMware Workstation; Image conversion; Converting from a physical to virtual environment; Summary; Chapter 3: Planning a Range; Planning; What are we trying to accomplish?; By when do we have to accomplish it?; Identifying vulnerabilities; Vulnerability sites; Vendor sites; Summary; Chapter 4: Identifying Range Architecture; Building the machines; Building new machines; Conversion; Cloning a virtual machine; Selecting network connections; The bridged setting; Network Address Translation; The host-only switch; The custom settings; Choosing range components The attacker machineRouter; Firewall; Web server; Summary; Chapter 5: Identifying a Methodology; The OSSTMM; The Posture Review; Logistics;

Active detection verification; Visibility Audit; Access verification; Trust verification; Control verification; Process verification; Configuration verification; Property validation; Segregation review; Exposure verification; Competitive intelligence scouting; Quarantine verification; Privileges audit; Survivability validation; Alert and log review; CHECK; NIST SP-800-115; The information security assessment methodology; Technical assessment techniques
Comparing tests and examinationsTesting viewpoints; Overt and covert; Offensive Security; Other methodologies; Customization; Summary; Chapter 6: Creating an External Attack Architecture; Establishing layered architectures; Configuring firewall architectures; iptables; Deploying IDS/IPS and load balancers; Intrusion Detection System (IDS); Intrusion Prevention System (IPS); Load balancers; Integrating web application firewalls; Summary; Chapter 7: Assessment of Devices; Assessing routers; Evaluating switches; MAC attacks; VLAN hopping attacks; GARP attacks; Attacking the firewall
Identifying the firewall rulesTricks to penetrate filters; Summary; Chapter 8: Architecting an IDS/IPS Range; Deploying a network-based IDS; Implementing the host-based IDS and endpoint security; Working with virtual switches; Evasion; Determining thresholds; Stress testing; Shell code obfuscation; Summary; Chapter 9: Assessment of Web Servers and Web Applications; Analyzing the OWASP Top Ten attacks; Injection flaws; Broken authentication and session management; Cross-Site Scripting; Insecure direct object references; Security misconfiguration; Sensitive data exposure
Missing function-level access control

Sommario/riassunto

Written in an easy-to-follow approach using hands-on examples, this book helps you create virtual environments for advanced penetration testing, enabling you to build a multi-layered architecture to include firewalls, IDS/IPS, web application firewalls, and endpoint protection, which is essential in the penetration testing world. If you are a penetration tester, security consultant, security test engineer, or analyst who wants to practice and perfect penetration testing skills by building virtual pen testing labs in varying industry scenarios, this is the book for you. This book is ideal if yo