1. Record Nr. UNINA9910790080203321

Autore	Ali Shakeel
Titolo	BackTrack 4 [[electronic resource]] : assuring security by penetration testing : master the art of penetration testing with BackTrack / / Shakeel Ali, Tedi Heriyanto
Pubbl/distr/stampa	Birmingham, U.K., : Packt Open Source, 2011
ISBN	1-283-37675-X 9786613376756 1-84951-395-3
Edizione	[1st edition]
Descrizione fisica	1 online resource (599 p.)
Collana	Community experience distilled
Altri autori (Persone)	HeriyantoTedi
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security - Evaluation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	BackTrack 4: Assuring Security by Penetration Testing; BackTrack 4: Assuring Security by Penetration Testing; Credits; About the Authors; About the Reviewers; www.PacktPub.com; Support files, eBooks, discount offers and more; Why Subscribe?; Free Access for Packt account holders; Preface; What this book covers; What you need for this book; Who this book is for; Conventions; Reader feedback; Customer support; Errata; Piracy; Questions; I. Lab Preparation and Testing Procedures; 1. Beginning with BackTrack; History; BackTrack purpose; Getting BackTrack; Using BackTrack; Live DVD Installing to hard diskInstallation in real machine; Installation in VirtualBox; Portable BackTrack; Configuring network connection; Ethernet setup; Wireless setup; Starting the network service; Updating BackTrack; Updating software applications; Updating the kernel; Installing additional weapons; Nessus vulnerability scanner; WebSecurify; Customizing BackTrack; Summary; 2. Penetration Testing Methodology; Types of penetration testing; Black-box testing; White-box testing; Vulnerability assessment versus penetration testing; Security testing methodologies Open Source Security Testing Methodology Manual (OSSTMM)Key features and benefits; Information Systems Security Assessment

Framework (ISSAF); Key features and benefits; Open Web Application Security Project (OWASP) Top Ten; Key features and benefits; Web Application Security Consortium Threat Classification (WASC-TC); Key features and benefits; BackTrack testing methodology; Target scoping; Information gathering; Target discovery; Enumerating target; Vulnerability mapping; Social engineering; Target exploitation; Privilege escalation; Maintaining access; Documentation and reporting
The ethicsSummary; II. Penetration Testers Armory; 3. Target Scoping; Gathering client requirements; Customer requirements form; Deliverables assessment form; Preparing the test plan; Test plan checklist; Profiling test boundaries; Defining business objectives; Project management and scheduling; Summary; 4. Information Gathering; Public resources; Document gathering; Metagoofil; DNS information; dnswalk; dnsenum; dnsmap; dnsmap-bulk; dnsrecon; fierce; Route information; 0trace; dmitry; itrace; tcpraceroute; tctrace; Utilizing search engines; goorecon; theharvester
All-in-one intelligence gatheringMaltego; Documenting the information; Dradis; Summary; 5. Target Discovery; Introduction; Identifying the target machine; ping; arping; arping2; fping; genlist; hping2; hping3; lanmap; nbtscan; nping; onesixtyone; OS fingerprinting; p0f; xprobe2; Summary; 6. Enumerating Target; Port scanning; AutoScan; Netifera; Nmap; Nmap target specification; Nmap TCP scan options; Nmap UDP scan options; Nmap port specification; Nmap output options; Nmap timing options; Nmap scripting engine; Unicornscan; Zenmap; Service enumeration; Amap; Httprint; Httsquash VPN enumeration

Sommario/riassunto

Master the art of penetration testing with BackTrack