Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition

Cardwell, Kevin,
author

Packt Publishing, Limited,
Aug. 2016

Electronic books

Monografía

Learn how to build complex virtual architectures that allow you to perform virtually any required testing methodology and perfect itAbout This Book Explore and build intricate architectures that allow you to emulate an enterprise network Test and enhance your security skills against complex and hardened virtual architecture Learn methods to bypass common enterprise defenses and leverage them to test the most secure environments. Who This Book Is ForWhile the book targets advanced penetration testing, the process is systematic and as such will provide even beginners with a solid methodology and approach to testing. You are expected to have network and security knowledge. The book is intended for anyone who wants to build and enhance their existing professional security and penetration testing methods and skills. What You Will Learn Learning proven security testing and penetration testing techniques Building multi-layered complex architectures to test the latest network designs Applying a professional testing methodology Determining whether there are filters between you and the target and how to penetrate them Deploying and finding weaknesses in common firewall architectures. Learning advanced techniques to deploy against hardened environments Learning methods to circumvent endpoint protection controls In DetailSecurity flaws and new hacking techniques emerge overnight security professionals need to make sure they always have a way to keep . With this practical guide, learn how to build your own virtual pentesting lab environments to practice and develop your security skills. Create challenging environments to test your abilities, and overcome them with proven processes and methodologies used by global penetration testing teams. Get to grips with the techniques needed to build complete virtual machines perfect for pentest training. Construct and attack layered architectures, and plan specific attacks based on the platforms you're going up against. Find new vulnerabilities for different kinds of systems and networks, and what these mean for your clients. Driven by a proven penetration testing methodology that has trained thousands of testers, Building Virtual Labs for Advanced Penetration Testing, Second Edition will prepare you for participation in professional security teams. Style and approach The book is written in an easy-to-follow format that provides a stepby-step, process-centric approach. Additionally, there are numerous hands-on examples and additional references for readers who might want to learn even more. The process developed throughout the book has been used to train and build teams all around the world as professional security and penetration testers

Título: Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition

Edición: 2nd ed

Editorial: Birmingham Packt Publishing, Limited Aug. 2016

Descripción física: 1 online resource

Contenido: Cover ; Credits; Copyright; About the Author; Acknowledgments; About the Reviewer; www. PacktPub.com; Table of Contents; Preface; Chapter 1: Introducing Penetration Testing ; Security testing; Authentication; Authorization; Confidentiality; Integrity; Availability; Non-repudiation; An abstract testing methodology; Planning; Nonintrusive target search; Nslookup; Central Ops; The Wayback Machine; Shodan; Intrusive target search; Find live systems; Discover open ports; Discover services; Enumeration; Identify vulnerabilities; Exploitation; Data analysis; Reporting; Description Analysis and exposureRecommendations; References; Myths and misconceptions about pen testing; Summary; Chapter 2: Choosing the Virtual Environment ; Open source and free environments; VMware Workstation Player; VirtualBox; Xen; Hyper-V; vSphere Hypervisor; Commercial environments; vSphere; XenServer; VMware Workstation Pro; Image conversion; Converting from a physical to a 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 Architectures 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 machine; Router; Firewall; Web server; Readers' challenge; 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 verificationProperty 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 examinations; Testing viewpoints; Overt and covert; Penetration Testing Execution Standard (PTES); Offensive Security; Other methodologies; Customization; Readers' challenge; Summary; Chapter 6: Creating an External Attack Architecture Configuring firewall architectures and establishing layered architecturesiptables; Testing; Adding a web server; Configuring the second layer; Setting the VLAN; Review pfSense; Deploying IDS; Intrusion Detection System (IDS); Readers' challenge; Summary; Chapter 7: Assessment of Devices ; Assessing routers; Router machine; Router scanning analysis; Verify our assumptions; Kali 2.0; iptables; Iptables network analysis; Evaluating switches; VLAN hopping attacks; GARP attacks; Layer two attack tool; Attacking the firewall; Tricks to penetrate filters; Readers' challenge; Summary

Copyright/Depósito Legal: 1076657219 1125073435

ISBN: 9781785883491 1785883496 Trade Paper) 9781785884955 ebk) 1785884956

Materia: Computer security- Testing Computer networks- Security measures Computers- Access control Computer networks- Security measures Computers- Access control

Enlace a formato físico adicional: Print version Cardwell, Kevin. Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition. Birmingham : Packt Publishing Ltd, 2016