1. Record Nr.	UNINA9910467467103321
Autore	Chebbi Chiheb
Titolo	Advanced Infrastructure Penetration Testing [[electronic resource] /] / Chebbi, Chiheb
Pubbl/distr/stampa	Packt Publishing, , 2018
Edizione	[1st edition]
Descrizione fisica	1 online resource (396 pages)
Soggetti	Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	A highly detailed guide to performing powerful attack vectors in many hands-on scenarios and defending significant security flaws in your company's infrastructure About This Book Advanced exploitation techniques to breach modern operating systems and complex network devices Learn about Docker breakouts, Active Directory delegation, and CRON jobs Practical use cases to deliver an intelligent endpoint-protected system Who This Book Is For If you are a system administrator, SOC analyst, penetration tester, or a network engineer and want to take your penetration testing skills and security knowledge to the next level, then this book is for you. Some prior experience with penetration testing tools and knowledge of Linux and Windows command-line syntax is beneficial. What You Will Learn Exposure to advanced infrastructure penetration testing techniques and methodologies Gain hands-on experience of penetration testing in Linux system vulnerabilities and memory exploitation Understand what it takes to break into enterprise networks Learn to secure the configuration management environment and continuous delivery pipeline Gain an understanding of how to exploit networks and IoT devices Discover real-world, post-exploitation techniques and countermeasures In Detail It has always been difficult to gain hands-on experience and a comprehensive understanding of advanced penetration testing techniques and vulnerability assessment and management. This book will be your one-stop solution to

compromising complex network devices and modern operating systems. This book provides you with advanced penetration testing techniques that will help you exploit databases, web and application servers, switches or routers, Docker, VLAN, VoIP, and VPN. With this book, you will explore exploitation abilities such as offensive PowerShell tools and techniques, CI servers, database exploitation, Active Directory delegation, kernel exploits, cron jobs, VLAN hopping, and Docker breakouts. Moving on, this book will not only walk you through managing vulnerabilities, but will also teach you how to ensure endpoint protection. Toward the end of this book, you will also discover post-exploitation tips, tools, and methodologies to help your organization build an intelligent security system. By the end of this book, you will have mastered the skills and methodologies needed to breach infrastructures and provide complete endpoint protection for your system. Style and approach Your one-stop...