1.

Record Nr.	UNINA9910818966703321
Autore	Chebbi Chiheb
Titolo	Mastering machine learning for penetration testing : develop an extensive skill set to break self-learning systems using Python / / Chiheb Chebbi
Pubbl/distr/stampa	Birmingham : , : Packt, , 2018
ISBN	1-78899-311-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (264 pages)
Disciplina	005.133
Soggetti	Python (Computer program language) Penetration testing (Computer security)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Sommario/riassunto	Become a master at penetration testing using machine learning with Python About This Book Identify ambiguities and breach intelligent security systems Perform unique cyber attacks to breach robust systems Learn to leverage machine learning algorithms Who This Book Is For This book is for pen testers and security professionals who are interested in learning techniques to break an intelligent security system. Basic knowledge of Python is needed, but no prior knowledge of machine learning is necessary. What You Will Learn Take an in-depth look at machine learning Get to know natural language processing (NLP) Understand malware feature engineering Build generative adversarial networks using Python libraries Work on threat hunting with machine learning and the ELK stack Explore the best practices for machine learning In Detail Cyber security is crucial for both businesses and individuals. As systems are getting smarter, we now see machine learning interrupting computer security. With the adoption of machine learning in upcoming security products, it's important for pentesters and security researchers to understand how these systems work, and to breach them for testing purposes. This book begins with the basics of machine learning and the algorithms used to build robust systems. Once you've gained a fair understanding of how security products

leverage machine learning, you'll dive into the core concepts of breaching such systems. Through practical use cases, you'll see how to find loopholes and surpass a self-learning security system. As you make your way through the chapters, you'll focus on topics such as network intrusion detection and AV and IDS evasion. We'll also cover the best practices when identifying ambiguities, and extensive techniques to breach an intelligent system. By the end of this book, you will be well-versed with identifying loopholes in a self-learning security system and will be able to efficiently breach a machine learning system. Style and approach This book takes a step-by-step approach to identify the loop holes in a self-learning security system. You will be able to efficiently breach a machine learning system with the help of best practices towards the end of the book.