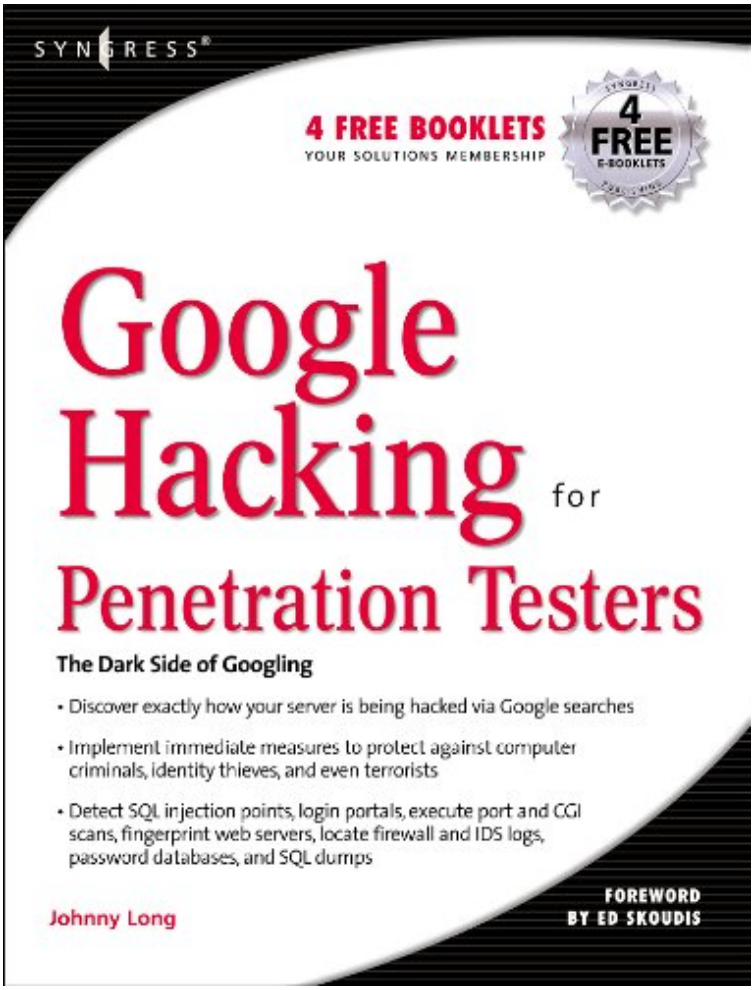
Google Hacking for Penetration Testers

Von Johnny Long
*ePub | *DOC | audiobook | ebooks | Download PDF*



Produktinformation -Verkaufsrang: #942661 in eBooksVerffentlicht am: 2004-12-17Erscheinungsdatum: 2004-12-17File Name: B0089EM5BG | File size: 48.Mb

Von Johnny Long : Google Hacking for Penetration Testers before purchasing it in order to gage whether or not it would be worth my time, and all praised Google Hacking for Penetration Testers:

KundenrezensionenHilfreichste Kundenrezensionen2 von 2 Kunden fanden die folgende Rezension hilfreich. Nice idea, but overloadedVon Gerhard AmonThe idea is great. Gain deep knowledge about the details of highly efficient Google-search-strings, then lean back and see the what people put on their websites: Excel-sheets with passwords, mail-server logs with tons of adresses etc.I think the book tells us: be careful! Google sees, finds and caches everything you put on the web, even if you think it will not be found.What is annoying with the book: sides full of search examples. After you have found your way through the Google search-parameters it definitevly makes no sense to cram the book full with loads of examples. Somehow I think the author had to achieve a minimum number of pages...? With regards to that, the price of the book seems high. You may visit the authors homepage to see the

examples there (and much more actual searches as well).1 von 1 Kunden fanden die folgende Rezension hilfreich. Google einmal andersVon Matthias HofherrDas Buch "Google Hacking for Penetration Testers" erfllt genau den versprochenen Rahmen: Es zeigt, wie Penetration Tester durch Suchanfragen bei Google interessante und sicherheitsrelevante Ergebnisse bzgl. ihres Ziels ermitteln knnen.Fr Nicht-Penetration-Tester sind die generellen Beschreibungen zur Nutzung der Google Search Engine sicher auch von Interesse, allerdings muss man sich dafr nicht unbedingt ein Buch dieser Preisklasse leisten.Einsteiger im Bereich Penetration Testing finden in diesem Buch zwingend notwendiges Wissen, das zum kleinen 1x1 eines PenTesters gehren sollte. Aber auch Profis knnen hier noch den einen oder anderen Trick lernen.Das Buch wird hervorragend ergnzt durch die Website des Autors, hier findet man eine durch die Community gut gepflegte Datenbank verschiedenster Google Suchmuster.2 von 3 Kunden fanden die folgende Rezension hilfreich. Holt mich nicht von den SockenVon Ein KundeDer Schwerpunkt dieses Buches sind die vielen ausfhrlichen Beispiele. Durch sie kann das Buch aber meiner Meinung nach nicht fehlenden inhaltichen Punkte ausgleichen. Im Grunde werden nur die Google-Funktionen ausfhrlich beleuchtet, welche man auch auf der Google-Homepage nachlesen kann. Mit den Beispielen wird das Buch dann eine unterhaltende Lektre, mehr aber auch nicht.Fazit: Fr Voyeure vielleicht interessant, aber um sich zum Thema Sicherheit weiterzubilden absolut ungeeignet.

KurzbeschreibungGoogle, the most popular search engine worldwide, provides web surfers with an easy-to-use guide to the Internet, with web and image searches, language translation, and a range of features that make web navigation simple enough for even the novice user. What many users dont realize is that the deceptively simple components that make Google so easy to use are the same features that generously unlock security flaws for the malicious hacker. Vulnerabilities in website security can be discovered through Google hacking, techniques applied to the search engine by computer criminals, identity thieves, and even terrorists to uncover secure information. This book beats Google hackers to the punch, equipping web administrators with penetration testing applications to ensure their site is invulnerable to a hackers search. Penetration Testing with Google Hacks explores the explosive growth of a technique known as "Google Hacking." When the modern security landscape includes such heady topics as "blind SQL injection" and "integer overflows," it's refreshing to see such a deceptively simple tool bent to achieve such amazing results; this is hacking in the purest sense of the word. Readers will learn how to torque Google to detect SQL injection points and login portals, execute port scans and CGI scans, fingerprint web servers, locate incredible information caches such as firewall and IDS logs, password databases, SQL dumps and much more - all without sending a single packet to the target! Borrowing the techniques pioneered by malicious "Google hackers," this talk aims to show security practitioners how to properly protect clients from this often overlooked and dangerous form of information leakage.*First book about Google targeting IT professionals and security leaks through web browsing. *Author Johnny Long, the authority on Google hacking, will be speaking about "Google Hacking" at the Black Hat 2004 Briefing. His presentation on penetrating security flaws with Google is expected to create a lot of buzz and exposure for the topic. *Johnny Long's Web site hosts the largest repository of Google security exposures and is the most popular destination for security professionals who want to learn about the dark side of Google.KurzbeschreibungGoogle, the most popular search engine worldwide, provides web surfers with an easy-to-use guide to the Internet, with web and image searches, language translation, and a range of features that make web navigation simple enough for even the novice user. What many users dont realize is that the deceptively simple components that make Google so easy to use are the same features that generously unlock security flaws for the malicious hacker. Vulnerabilities in website security can be discovered through Google hacking, techniques applied to the search engine by computer criminals, identity thieves, and even terrorists to uncover secure information. This book beats Google hackers to the punch, equipping web administrators with penetration testing applications to ensure their site is invulnerable to a hackers search. Penetration Testing with Google Hacks explores the explosive growth of a technique known as "Google Hacking." When the modern security landscape includes such heady topics as "blind SQL injection" and "integer overflows," it's refreshing to see such a deceptively simple tool bent to achieve such amazing results; this is hacking in the purest sense of the word. Readers will learn how to torque Google to detect SQL injection points and login portals, execute port scans and CGI scans, fingerprint web servers, locate incredible information caches such as firewall and IDS logs, password databases, SQL dumps and much more - all without sending a single packet to the target! Borrowing the techniques pioneered by malicious "Google hackers," this talk aims to show security practitioners how to properly protect clients from this often overlooked and dangerous form of information leakage.*First book about Google targeting IT professionals and security leaks through web browsing. *Author Johnny Long, the authority on Google hacking, will be speaking about "Google Hacking" at the Black Hat 2004 Briefing. His presentation on penetrating security flaws with Google is expected to create a lot of buzz and exposure for the topic. *Johnny Long's Web site hosts the largest repository of Google security exposures and is the most popular destination for security professionals who want to learn about the dark side of Google.Synopsis Google, the most popular search engine worldwide, provides web surfers with an easy-to-use guide to the Internet, with web

and image searches, language translation, and a range of features that make web navigation simple enough for even the novice user. What many users dont realize is that the deceptively simple components that make Google so easy to use are the same features that generously unlock security flaws for the malicious hacker. Vulnerabilities in website security can be discovered through Google hacking, techniques applied to the search engine by computer criminals, identity thieves, and even terrorists to uncover secure information.This book beats Google hackers to the punch, equipping web administrators with penetration testing applications to ensure their site is invulnerable to a hackers search. "Penetration Testing with Google Hacks" explores the explosive growth of a technique known as "Google Hacking." When the modern security landscape includes such heady topics as "blind SQL injection" and "integer overflows," it's refreshing to see such a deceptively simple tool bent to achieve such amazing results; this is hacking in the purest sense of the word.Readers will learn how to torque Google to detect SQL injection points and login portals, execute port scans and CGI scans, fingerprint web servers, locate incredible information caches such as firewall and IDS logs, password databases, SQL dumps and much more - all without sending a single packet to the target!Borrowing the techniques pioneered by malicious "Google hackers," this talk aims to show security practitioners how to properly protect clients from this often overlooked and dangerous form of information leakage.This is the first book about Google targeting IT professionals and security leaks through web browsing. Author Johnny Long, the authority on Google hacking, will be speaking about "Google Hacking" at the Black Hat 2004 Briefing. His presentation on penetrating security flaws with Google is expected to create a lot of buzz and exposure for the topic. Johnny Long's Web site hosts the largest repository of Google security exposures and is the most popular destination for security professionals who want to learn about the dark side of Google.