Hacking The Art Of Exploitation Jon Erickson

Yeah, reviewing a ebook Hacking The Art Of Exploitation Jon Erickson could build up your close contacts listings. This is just one of the solutions for you to be successful. As understood, completion does not recommend that you have fabulous points.

Comprehending as competently as union even more than extra will allow each success. next-door to, the declaration as with ease as keenness of this Hacking The Art Of Exploitation Jon Erickson can be taken as without difficulty as picked to act.

Adversarial Tradecraft in Cybersecurity Dan Borges 2021-06-14 Master cutting-edge techniques and countermeasures to protect your organization from live hackers. Learn how to harness cyber deception in your operations to gain an edge over the competition. Key FeaturesGain an advantage against live hackers in a competition or real computing environmentUnderstand advanced red team and blue team techniques with code examplesLearn to battle in short-term memory, whether remaining unseen (red teams) or monitoring an attacker's traffic (blue teams)Book Description Little has been written about what to do when live hackers are on your system and running amok. Even experienced hackers tend to choke up when they realize the network defender has caught them and is zoning in on their implants in real time. This book will provide tips and tricks all along the kill chain of an attack, showing where hackers can have the upper hand in a live conflict and how defenders can outsmart them in this adversarial game of computer cat and mouse. This book contains two subsections in each chapter, specifically focusing on the offensive and defensive teams. It begins by introducing you to adversarial operations and principles of computer conflict where you will explore the core principles of deception, humanity, economy, and more about human-on-human conflicts. Additionally, you will understand everything from planning to setting up infrastructure and tooling that both sides should have in place. Throughout this book, you will learn how to gain an advantage over opponents by disappearing from what they can detect. You will further understand how to blend in, uncover other actors' motivations and means, and learn to tamper with them to hinder their ability to detect your presence. Finally, you will learn how to gain an advantage through advanced research and thoughtfully concluding an operation. By the end of this book, you will have achieved a solid understanding of cyberattacks from both an attacker's and a defender's perspective. What you will learnUnderstand how to implement process injection and how to detect itTurn the tables on the offense with active defenseDisappear on the defender's system, by tampering with defensive sensorsUpskill in using deception with your backdoors and countermeasures including honeypotsKick someone else from a computer you are on and gain the upper handAdopt a language agnostic approach to become familiar with techniques that can be applied to both the red and blue teamsPrepare yourself for real-time cybersecurity conflict by using some of the best techniques currently in the industryWho this book is for Pentesters to red teamers, security operations center analysts to incident responders, attackers, defenders, general hackers, advanced computer users, and security engineers will benefit from this book. Participants in purple teaming or adversarial simulations will also learn a lot from its practical examples of processes for gaining an advantage over the opposing team. Basic knowledge of Python, Go, Bash, PowerShell, system administration as well as knowledge of incident response in Linux and prior exposure to any kind of cybersecurity knowledge, penetration testing, and ethical hacking basics will help you follow along.

Sieben Wochen, sieben Sprachen (Prags) Bruce A. Tate 2011-06-30 Mit diesen sieben Sprachen erkunden Sie die wichtigsten Programmiermodelle unserer Zeit. Lernen Sie die dynamische Typisierung kennen, die Ruby, Python und Perl so flexibel und verlockend macht. Lernen Sie das Prototyp-System verstehen, das das Herzstück von JavaScript bildet. Erfahren Sie, wie das Pattern Matching in Prolog die Entwicklung von Scala und Erlang beeinflusst hat. Entdecken Sie, wie sich die rein funktionale Programmierung in Haskell von der Lisp-Sprachfamilie, inklusive Clojure, unterscheidet. Erkunden Sie die parallelen Techniken, die das Rückgrat der nächsten Generation von Internet-Anwendungen bilden werden. Finden Sie heraus, wie man Erlangs "Lass es abstürzen"-Philosophie zum Aufbau fehlertoleranter Systeme nutzt. Lernen Sie das Aktor-Modell kennen, das das parallele Design bei Io und Scala bestimmt. Entdecken Sie, wie Clojure die Versionierung nutzt, um einige der schwierigsten Probleme der Nebenläufigkeit zu lösen. Hier finden Sie alles in einem Buch. Nutzen Sie die Konzepte einer Sprache, um kreative Lösungen in einer anderen Programmiersprache zu finden – oder entdecken Sie einfach eine Sprache, die Sie bisher nicht kannten. Man kann nie wissen – vielleicht wird sie sogar eines ihrer neuen Lieblingswerkzeuge.

Systemarchitektur zur Ein- und Ausbruchserkennung in verschlüsselten Umgebungen Robert Koch 2011 Das Internet hat sich mit einer beispiellosen Geschwindigkeit in den Lebensalltag integriert. Umfangreiche Dienste erm glichen es, Bestellungen, finanzielle Transaktionen, etc. ber das Netz durchzuf hren. Auch traditionelle Dienste migrieren mehr und mehr in das Internet, wie bspw. Telefonie oder Fernsehen. Die finanziellen Werte, die hierbei umgesetzt werden, haben eine hohe Anziehungskraft auf Kriminelle: Angriffe im Internet sind aus einer sicheren Entfernung heraus m glich, unterschiedliches IT-Recht der verschiedenen L nder erschwert die grenz berschreitende Strafverfolgung zus tzlich. Entsprechend hat sich in den letzten Jahren ein milliardenschwerer Untergrundmarkt im Internet etabliert. Um Systeme und Netze vor Angriffen zu sch tzen, befinden sich seit ber 30 Jahren Verfahren zur Einbruchsdetektion in der Erforschung. Zahlreiche Systeme sind auf dem Markt verf gbar und geh ren heute zu den Sicherheitsmechanismen jedes gr eren Netzes. Trotz dieser Anstrengungen nimmt die Zahl von Sicherheitsvorf llen nicht ab, sondern steigt weiterhin an. Heutige Systeme sind nicht in der Lage, mit Herausforderungen wie zielgerichteten Angriffen, verschl sselten Datenleitungen oder Innent tern umzugehen. Der Beitrag der vorliegenden Dissertation ist die Entwicklung einer Architektur zur Ein- und Ausbruchserkennung in verschl sselten Umgebungen. Diese beinhaltet sowohl Komponenten zur Erkennung von extern durchgef hrten Angriffen, als auch zur Identifikation von Innent tern. Hierbei werden statistische Methoden auf Basis einer verhaltensbasierten Detektion genutzt, so dass keine Entschl sselung des Datenverkehrs erforderlich ist. Im Gegensatz zu bisherigen Methoden ben tigt das System hierbei keine Lernphasen. Ausgehend von einem Szenario der IT-Struktur heutiger Unternehmen werden die Anforderungen an ein System zur Ein- und Ausbruchserkennung definiert. Da eine Detektion die Kenntnis entsprechender, messbarer Ansatzpunkte ben tigt, erfolgt eine detaillierte Analyse ein

Hacking Jon Erickson 2003 Describes the techniques of computer hacking, covering such topics as stack-based overflows, format string exploits, and shellcode.

Die Xbox hacken. Andrew Huang 2004

Hacken für Dummies Kevin Beaver 2019-01-14 Um einen Hacker zu überlisten, müssen Sie sich in die Denkweise des Hackers hineinversetzen. Deshalb lernen Sie mit diesem Buch, wie ein Bösewicht zu denken. Der Fachmann für IT-Sicherheit Kevin Beaver teilt mit Ihnen sein Wissen über Penetrationstests und typische Schwachstellen in IT-Systemen. Er zeigt Ihnen, wo Ihre Systeme verwundbar sein könnten, sodass Sie im Rennen um die IT-Sicherheit die Nase vorn behalten. Denn wenn Sie die Schwachstellen in Ihren Systemen kennen, können Sie sie besser schützen und die Hacker kommen bei Ihnen nicht zum Zug!

Der LEGO®-Architekt Tom Alphin 2017-09-08 Werde LEGO®-Architekt! Begebe dich auf eine Reise durch die Architekturgeschichte: Lerne Baustile vom Neoklassizismus über Modernismus bis hin zu High-Tech-Lösungen kennen – verwirklicht mit LEGO. Anleitungen für 12 Modelle in verschiedenen Architekturstilen laden zum Nachbau ein und inspirieren dich zu eigenen Bauwerken. Dieses Buch ist von der LEGO-Gruppe weder unterstützt noch autorisiert worden.

Mehr Hacking mit Python Justin Seitz 2015-10-09 Wenn es um die Entwicklung leistungsfähiger und effizienter Hacking-Tools geht, ist Python für die meisten Sicherheitsanalytiker die Sprache der Wahl. Doch wie genau funktioniert das? In dem neuesten Buch von Justin Seitz - dem Autor des Bestsellers "Hacking mit Python" - entdecken Sie Pythons dunkle Seite. Sie entwickeln Netzwerk-Sniffer, manipulieren Pakete, infizieren virtuelle Maschinen, schaffen unsichtbare Trojaner und vieles mehr. Sie lernen praktisch, wie man • einen "Command-and-Control"-Trojaner mittels GitHub schafft • Sandboxing erkennt und gängige Malware-Aufgaben wie Keylogging und Screenshotting automatisiert • Windows-Rechte mittels kreativer Prozesskontrolle ausweitet • offensive Speicherforensik-Tricks nutzt, um Passwort-Hashes abzugreifen und Shellcode in virtuelle Maschinen einzuspeisen • das beliebte Web-Hacking-Tool Burp erweitert • die Windows COM-Automatisierung nutzt, um einen Man-in-the-Middle-Angriff durchzuführen • möglichst unbemerkt Daten aus einem Netzwerk abgreift Eine Reihe von Insider-Techniken und kreativen Aufgaben zeigen Ihnen, wie Sie die Hacks erweitern und eigene Exploits entwickeln können.

Hacking Jon Erickson 2008

Twitter Nick Bilton 2013-11-01 Kontakt zu Freunden halten - das ist eine der Ideen hinter Twitter. Doch einer der Gründer erreichte für sich persönlich das Gegenteil: Intrigen machten aus Kumpeln bittere Feinde. "New York Times"-Reporter Nick Bilton hat darüber jetzt ein Buch geschrieben. Twitter wächst, trotz technischer Probleme, aber wer sich dafür näher interessiert, ist bei Nick Bilton falsch aufgehoben: Hier geht es um die Egokämpfe und Machtspiele, nicht um Feinheiten der Serversteuerung oder der Medienrevolution.

Ending Spam Jonathan A. Zdziarski 2005 Explains how spam works, how network administrators can implement spam filters, or how programmers can develop

new remarkably accurate filters using language classification and machine learning. Original. (Advanced)

Hacking- The art Of Exploitation J. Erickson 2018-03-06 This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

Hacking mit Metasploit Michael Messner 2017-11-28 Metasploit ist ein Penetration-Testing-Werkzeug, das in der Toolbox eines jeden Pentesters zu finden ist. Dieses Buch stellt das Framework detailliert vor und zeigt, wie Sie es im Rahmen unterschiedlichster Penetrationstests einsetzen. Am Beispiel von Metasploit erhalten Sie einen umfassenden Einblick ins Penetration Testing. Sie lernen typische Pentesting-Tätigkeiten kennen und können nach der Lektüre komplexe, mehrstufige Angriffe vorbereiten, durchführen und protokollieren. Jeder dargestellte Exploit bzw. jedes dargestellte Modul wird anhand eines praktischen Anwendungsbeispiels in einer gesicherten Laborumgebung vorgeführt. Behandelt werden u.a. folgende Themen: • Komplexe, mehrstufige Penetrationstests • Post-Exploitation-Tätigkeiten • Metasploit-Erweiterungen • Webapplikationen, Datenbanken, Client-Side-Angriffe, IPv6 • Automatisierung mit Ruby-Skripten • Entwicklung eigener Exploits inkl. SEHExploits • Exploits für Embedded Devices entwickeln • Umgehung unterschiedlichster Sicherheitsumgebungen Die dritte Auflage wurde überarbeitet und aktualisiert. Neu dabei: • Post-Exploitation-Tätigkeiten mit Railgun vereinfachen • Bad-Characters bei der Entwicklung von Exploits berücksichtigen • Den Vulnerable Service Emulator nutzen Vorausgesetzt werden fundierte Kenntnisse der Systemtechnik (Linux und Windows) sowie der Netzwerktechnik.

Hello World Hannah Fry 2019-03-14 Weitere Informationen zum Buch und zur Autorin finden Sie beim Special Sie sind eines Verbrechens angeklagt. Wer soll über Ihr Schicksal entscheiden? Ein menschlicher Richter oder ein Computer-Algorithmus? Sie sind sich absolut sicher? Sie zögern womöglich? In beiden Fällen sollten Sie das Buch der jungen Mathematikerin und Moderatorin Hannah Fry lesen, das mit erfrischender Direktheit über Algorithmen aufklärt, indem es von Menschen handelt. Algorithmen prägen in wachsendem Ausmaß den Alltag von Konsum, Finanzen, Medizin, Polizei, Justiz, Demokratie und sogar Kunst. Sie sortieren die Welt für uns, eröffnen neue Optionen und nehmen uns Entscheidungen ab - schnell, effektiv, gründlich. Aber sie tun das, ohne zu fragen, und stellen uns vor neue Dilemmata. Vor allem jedoch: Wir neigen dazu, Algorithmen als eine Art Autorität zu betrachten. statt ihre Macht infrage zu stellen. Keine Dimension unserer Welt, in der sie nicht längst Einzug gehalten haben: Algorithmen, diese unscheinbaren Folgen von Anweisungen, die im Internet sowieso, aber auch in jedem Computerprogramm tätig sind, prägen in wachsendem, beängstigendem Ausmaß den Alltag von Konsum, Finanzen, Medizin, Polizei, Justiz, Demokratie und sogar Kunst. Sie sortieren die Welt für uns, eröffnen neue Optionen und nehmen uns Entscheidungen ab - schnell, effektiv, gründlich. Aber sie tun das häufig, ohne uns zu fragen, und sie stellen uns vor neue, keineswegs einfach zu lösende Dilemmata. Vor allem aber: Wir neigen dazu, Algorithmen als eine Art Autorität zu betrachten, statt ihre Macht in Frage zu stellen. Das öffnet Menschen, die uns ausbeuten wollen, Tür und Tor. Es verhindert aber auch, dass wir bessere Algorithmen bekommen. Solche, die uns bei Entscheidungen unterstützen, anstatt über uns zu verfügen. Die offenlegen, wie sie zu einer bestimmten Entscheidung gelangen. Demokratische, menschliche Algorithmen. Dafür plädiert dieses Buch - zugänglich, unterhaltsam, hochinformativ.

Wicked Cool Java Brian D. Eubanks 2005 Containing 101 fun, interesting, and useful ways to get more out of Java, this title targets developers and system architects who have some basic Java knowledge but may not be familiar with the wide range of libraries available.

Hacking Eric Amberg / Daniel Schmid 2021-12-07 • Methoden und Tools der Hacker, Cyberkriminellen und Penetration Tester • Mit zahlreichen Schritt-für-Schritt-Anleitungen und Praxis-Workshops • Inklusive Vorbereitung auf den Certified Ethical Hacker (CEHv11) mit Beispielfragen zum Lernen Dies ist ein praxisorientierter Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheitsspezialisten und interessierte Poweruser. Mithilfe vieler Workshops, Schritt-für-Schritt-Anleitungen sowie Tipps und Tricks lernen Sie unter anderem die Werkzeuge und Mittel der Hacker und Penetration Tester sowie die Vorgehensweise eines professionellen Hacking-Angriffs kennen. Der Fokus liegt auf der Perspektive des Angreifers und auf den Angriffstechniken, die jeder Penetration Tester kennen muss. Dabei erläutern die Autoren für alle Angriffe auch effektive Gegenmaßnahmen. So gibt dieses Buch Ihnen zugleich auch schrittweise alle Mittel und Informationen an die Hand, um Ihre Systeme auf Herz und Nieren zu prüfen, Schwachstellen zu erkennen und sich vor Angriffen effektiv zu schützen. Das Buch umfasst nahezu alle relevanten Hacking-Themen und besteht aus sechs Teilen zu den Themen: Arbeitsumgebung, Informationsbeschaffung, Systeme angreifen, Netzwerk- und sonstige Angriffe, Web Hacking sowie Angriffe auf WLAN und Next-Gen-Technologien. Jedes Thema wird systematisch erläutert. Dabei werden sowohl die Hintergründe und die zugrundeliegenden Technologien als auch praktische Beispiele in konkreten Szenarien besprochen. So haben Sie die Möglichkeit, die Angriffstechniken selbst zu erleben und zu üben. Das Buch ist als Lehrbuch konzipiert, eignet sich aber auch als Nachschlagewerk. Sowohl der Inhalt als auch die Methodik orientieren sich an der Zertifizierung zum Certified Ethical Hacker (CEHv11) des EC-Council. Testfragen am Ende jedes Kapitels helfen dabei, das eigene Wissen zu überprüfen und für die CEH-Prüfung zu trainieren. Damit eignet sich das Buch hervorragend als ergänzendes Material zur Prüfungsvorbereitung. Aus dem Inhalt: • Aufbau einer HackingLaborumgebung • Einführung in Kali Linux als Hacking-Plattform • Sicher und anonym im Internet kommunizieren • Reconnaissance (Informationsbeschaffung) • Vulnerability-Scanning • Password Hacking • Bind und Reverse Shells • Mit Maiware das System übernehmen • Spuren verwischen • Lauschangriffe und Man-in-the-Middle • Social Engineering • Web- und WLAN-Hacking • Angriffe auf IoT-Systeme • Cloud-Hacking und -Security • Durchführen von Penetrationstests

Python kinderleicht! Jason Briggs 2016-03-09 Python ist eine leistungsfähige, moderne Programmiersprache. Sie ist einfach zu erlernen und macht Spaß in der Anwendung – mit diesem Buch umso mehr! "Python kinderleicht" macht die Sprache lebendig und zeigt Dir (und Deinen Eltern) die Welt der Programmierung. Jason R. Briggs führt Dich Schritt für Schritt durch die Grundlagen von Python. Du experimentierst mit einzigartigen (und oft urkomischen) Beispielprogrammen, bei denen es um gefräßige Monster, Geheimagenten oder diebische Raben geht. Neue Begriffe werden erklärt, der Programmcode ist farbig dargestellt, strukturiert und mit Erklärungen versehen. Witzige Abbildungen erhöhen den Lernspaß. Jedes Kapitel endet mit Programmier-Rätseln, an denen Du das Gelernte üben und Dein Verständnis vertiefen kannst. Am Ende des Buches wirst Du zwei komplette Spiele programmiert haben: einen Klon des berühmten "Pong" und "Herr Strichmann rennt zum Ausgang" – ein Plattformspiel mit Sprüngen, Animation und vielem mehr. Indem Du Seite für Seite neue Programmierabenteuer bestehst, wirst Du immer mehr zum erfahrenen Python-Programmierer. - Du lernst grundlegende Datenstrukturen wie Listen, Tupel und Maps kennen. - Du erfährst, wie man mit Funktionen und Modulen den Programmcode organisieren und wiederverwenden kann. - Du wirst mit Kontrollstrukturen wie Schleifen und bedingten Anweisungen vertraut und lernst, mit Objekten und Methoden umzugehen. - Du zeichnest Formen mit dem Python-Modul Turtle und erstellst Spiele, Animationen und andere grafische Wunder mit tkinter. Und: "Python kinderleicht" macht auch für Erwachsene das Programmierenlernen zum Kinderspiel! Alle Programme findest Du auch zum Herunterladen auf der Website!

Die Kunst der Anonymität im Internet Kevin D. Mitnick 2017-11-24 Ob Sie wollen oder nicht – jede Ihrer Online-Aktivitäten wird beobachtet und analysiert Sie haben keine Privatsphäre. Im Internet ist jeder Ihrer Klicks für Unternehmen, Regierungen und kriminelle Hacker uneingeschränkt sichtbar. Ihr Computer, Ihr Smartphone, Ihr Auto, Ihre Alarmanlage, ja sogar Ihr Kühlschrank bieten potenzielle Angriffspunkte für den Zugriff auf Ihre Daten. Niemand kennt sich besser aus mit dem Missbrauch persönlicher Daten als Kevin Mitnick. Als von der US-Regierung ehemals meistgesuchter Computer-Hacker kennt er alle Schwachstellen und Sicherheitslücken des digitalen Zeitalters. Seine Fallbeispiele sind spannend und erschreckend: Sie werden Ihre Aktivitäten im Internet neu überdenken. Mitnick weiß aber auch, wie Sie Ihre Daten bestmöglich schützen. Er zeigt Ihnen anhand zahlreicher praktischer Tipps und Schritt-für-Schritt-Anleitungen, was Sie tun können, um online und offline anonym zu sein. Bestimmen Sie selbst über Ihre Daten. Lernen Sie, Ihre Privatsphäre im Internet zu schützen. Kevin Mitnick zeigt Ihnen, wie es geht. Hinterlassen Sie keine Spuren ? Sichere Passwörter festlegen und verwalten ? Mit dem Tor-Browser im Internet surfen, ohne Spuren zu hinterlassen ? E-Mails und Dateien verschlüsseln und vor fremden Zugriffen schützen ? Öffentliches WLAN, WhatsApp, Facebook & Co. sicher nutzen ? Sicherheitsrisiken vermeiden bei GPS, Smart-TV, Internet of Things und Heimautomation ? Eine zweite Identität anlegen und unsichtbar werden

Security Data Visualization Greg Conti 2007 An introduction to a range of cyber security issues explains how to utilize graphical approaches to displaying and understanding computer security data, such as network traffic, server logs, and executable files, offering guidelines for identifying a network attack, how to assess a system for vulnerabilities with Afterglow and RUMINT visualization software, and how to protect a system from additional attacks. Original. (Intermediate)

Morgen ist heute gestern Mark Stevenson 2012-06-04 Wie die Welt in 1000 Jahren aussehen wird, können wir nur vermuten. Wie dramatisch aber Technik, Wissenschaft und Forschung unser Leben in den kommenden zehn Jahren verändern werden, das hat Mark Stevenson herausgefunden. Und er nimmt uns mit auf eine atemberaubende Tour in die nächste Zukunft: Dort begegnen wir sozial agierenden Robotern (die gleichwohl unter Stimmungsschwankungen leiden), lernen Transhumanisten kennen (die eifrig auf das tausendjährige Leben hinarbeiten), touren mit Spaceshuttles durch die Wüste und entschlüsseln die Geheimnisse der Nanotechnologie. Dabei propagiert Stevenson keineswegs einen blinden Optimismus, sondern öffnet uns die Augen für die unfassbaren Möglichkeiten, die wir haben. Sein Fazit: Die besten Jahre liegen noch vor uns, freuen wir uns drauf!

Write Portable Code Brian Hook 2005 Contains lessons on cross-platform software development, covering such topics as portability techniques, source control, compilers, user interfaces, and scripting languages.

Die Frau mit den Eiern 2004

The Art of Network Penetration Testing Royce Davis 2020-12-29 The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. Summary Penetration testing is about more than just getting through a perimeter firewall. The biggest security threats are inside the network, where attackers can rampage through sensitive data by exploiting weak access controls and poorly patched software. Designed for up-and-coming security professionals, The Art of Network Penetration Testing teaches you how to take over an enterprise network from the inside. It lays out every stage of an internal security assessment step-by-step, showing you how to identify weaknesses before a malicious invader can do real damage. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Penetration testers uncover security gaps by attacking networks exactly like malicious intruders do. To become a world-class pentester, you need to master offensive security concepts, leverage a proven methodology, and practice, practice, practice. Th is book delivers insights from security expert Royce Davis, along with a virtual testing environment you can use to hone your skills. About the book The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. As you brute force passwords, exploit unpatched services, and elevate network level privileges, you'll learn where the weaknesses are—and how to take advantage of them. What's inside Set up a virtual pentest lab Exploit Windows and Linux network vulnerabilities Establish persistent re-entry to compromised targets Detail your findings in an engagement report About the reader For tech professionals. No security experience required. About the author Royce Davis has orchestrated hundreds of penetration tests, helping to secure many of the largest companies in the world. Table of Contents 1 Network Penetration Testing PHASE 1 - INFORMATION GATHERING 2 Discovering network hosts 3 Discovering network services 4 Discovering network vulnerabilities PHASE 2 - FOCUSED PENETRATION 5 Attacking vulnerable web services 6 Attacking vulnerable database services 7 Attacking unpatched services PHASE 3 - POST-EXPLOITATION AND PRIVILEGE ESCALATION 8 Windows post-exploitation 9 Linux or UNIX post-exploitation 10 Controlling the entire network PHASE 4 - DOCUMENTATION 11 Post-engagement cleanup 12 Writing a solid pentest deliverable

Cyberdeterrence and Cyberwar Martin C. Libicki 2009-09-22 Cyberspace, where information--and hence serious value--is stored and manipulated, is a tempting target. An attacker could be a person, group, or state and may disrupt or corrupt the systems from which cyberspace is built. When states are involved, it is tempting to compare fights to warfare, but there are important differences. The author addresses these differences and ways the United States protect itself in the face of attack.

Die Kunst des Einbruchs Kevin Mitnick 2012-07-10 Kevin Mitnick, einst der meistgesuchte Verbrecher der USA, saß fünf Jahre im Gefängnis, weil er in zahlreiche Netzwerke großer Firmen eingebrochen war. Heute ist er rehabilitiert, gilt aber nach wie vor weltweit als Prototyp des Hackers. Seit längerer Zeit hat Mitnick in der Hackerszene nach authentischen und spannenden Geschichten gesucht, die auch für Sicherheitsverantwortliche in Firmen hoch-interessante Erkenntnisse abwerfen. Die hier vorliegende Sammlung von Geschichten ist das Ergebnis dieser Suche. „Tauchen Sie aus der Sicherheit und Geborgenheit Ihres Lesesessels ein in die feindselige Welt der Computerkriminalität. Mitnick präsentiert zehn packende Kapitel, jedes das Ergebnis eines Interviews mit einem echten Hacker, der von einem echten Angriff erzählt. Pflichtlektüre für jeden, der sich für Computersicherheit interessiert." Tom Parker, Computer-Sicherheitsanalytiker und Gründer der Global InterSec LLC

Hacking VoIP Himanshu Dwivedi 2009 Voice over Internet Protocol (VoIP) networks, the technology used to place phone calls through the Internet, suffer from the same security holes as standard IP networks. This book reviews the many possible VoIP attacks, and discusses the best defenses against them.

Hacking und IT-Security für Einsteiger Max Engelhardt 2020

Network Know-How John Ross 2009 A guide to creating a home computer network covers such topics as implementing network addressing, configuring network adapters and routers, sharing music and photos, automating household appliances, and troubleshooting.

The Book of Postfix Ralf Hildebrandt 2005 A guide to using Postfix covers such topics as filtering spam and viruses, authenticating users, encrypting with TLC, and setting up mail gateways.

Command and Control Eric Schlosser 2013-09-30 Arkansas, 18. September 1980, abends: Bei Routinearbeiten an einer gefechtsbereiten Titan-II-Rakete rutscht einem Arbeiter ein Schraubenschlüssel aus der Hand. »O Mann, das ist nicht gut", ist sein erster Gedanke. Das Missgeschick führt zu einer Kettenreaktion, der größte je gebaute Atomsprengkopf droht zu explodieren ... Weltweit sind Tausende von Atomsprengköpfen stationiert. Viele von ihnen werden rund um die Uhr gefechtsbereit gehalten, damit sie innerhalb einer Minute starten und eine unvorstellbare Verwüstung anrichten können. Was das für die Soldaten in den unterirdischen Bunkern heißt und welche Gefahren von den scharfen Atomwaffen ausgehen, ist uns kaum bewusst. Der Journalist und Bestseller-Autor Eric Schlosser deckt in diesem zeithistorischen Thriller auf der Grundlage von geheimen Unterlagen des Verteidigungsministeriums und Interviews mit Augenzeugen einen dramatischen Unfall in einem Atomwaffensilo der USA auf, der um ein Haar mehrere amerikanische Großstädte vernichtet hätte. In diesen Krimi einer am Ende gerade noch gelungenen Rettung flicht er die Geschichte der amerikanischen Atomrüstung ein. Er erzählt, wie Raketen und Sprengköpfe rund um die Uhr abschussbereit gehalten werden und wie die Menschen ticken, die ihr Leben für die Sicherheit der Massenvernichtungswaffen einsetzen. Eine spektakuläre Geschichte des Kalten Krieges und der Atomrüstung «von unten»: aus der Sicht der Soldaten in den Silos, die mit einem falschen Handgriff die Apokalypse auslösen können. «Atemberaubend, ... mitreißend ... Eric Schlosser verbindet profunde Informationen mit der Erzählung haarsträubender Details zu zahlreichen Unfällen und zeigt, dass auch die besten Kontrollsysteme nicht menschlichen Fehlern, Missgeschicken und der wachsenden technologischen Komplexität gewachsen sind.» Publisher's Weekly »Ebenso anschaulich wie erschütternd ... Eine umfassende und beunruhigende Untersuchung über die Illusion der Sicherheit von Atomwaffen." Kirkus Reviews «Die weltweiten Atwomwaffenarsenale sind nicht so sicher, wie sie sein sollten – das ist die Botschaft dieses faszinierenden und aufwühlenden Buches.» Lee H. Hamilton, ehemaliger Kongress-Abgeordneter der USA und Co-Vorsitzender der Blue Ribbon Commission on America's Nuclear Future

Autotools John Calcote 2010 The GNU Autotools make it easy for developers to create software that is portable across many UNIX-like operating systems. Thousands of open source software packages use the Autotools, but the learning curve is unfortunately steep, and it can be difficult for a beginner to find anything more than basic reference material on using the powerful software suite. InAutotools, author John Calcote begins with an overview of high-level concepts; then tackles more advanced topics, like using the M4 macro processor with Autoconf, extending the Automake framework, and building Java and C# sources. You'll learn how to: Master the Autotools build system to maximize your software's portability Generate Autoconf configuration scripts to simplify the compilation process Produce portable makefiles with Automake Build cross-platform software libraries with Libtool Write your own Autoconf macros Autotoolsalso includes a variety of complete projects that you're encouraged to work through to gain a real-world sense of how to become an Autotools practitioner. For example, you'll turn the FLAIM and Jupiter projects' hand-coded, makefile-based build systems into a powerful Autotools-based build system.

PHP & MySQL von Kopf bis Fuß Lynn Beighley 2009

BIG SHOTS ! Henry Carroll 2015-01 Keine komplizierten Kurven. Keine technischen Diagramme. "BIG SHOTS!" führt Sie durch die Grundlagen von Komposition, Belichtung, Licht, Objektiven und Bildgestaltung, ohne Sie mit Technikgefasel zu langweilen. Dieses Buch richtet sich an Einsteiger und Profis und eignet sich für Besitzer von Kompakt- und DSLR-Kameras. Randvoll mit praktischen Tipps und Techniken, die sich sofort in Ihren Fotos zeigen. Mit einer Auswahl der besten Aufnahmen von 50 renommierten Fotografen von Weltrang, die dazu inspirieren, selbst zur Kamera zu greifen.

Inside Anonymous Parmy Olson 2012-07-06 Erstmals packen die Hacker aus. Ende des Jahres 2010 nahmen weltweit Tausende an den digitalen Angriffen der Hackergruppe Anonymous auf die Webseiten von VISA, MasterCard und PayPal teil, um gegen die Sperrung der Konten von Wiki-Leaks zu protestieren. Splittergruppen von Anonymous infiltrierten die Netzwerke der totalitären Regime von Libyen und Tunesien. Eine Gruppe namens LulzSec schaffte es sogar, das FBI, die CIA und Sony zu attackieren, bevor sie sich wieder auflöste. Das Anonymous-Kollektiv wurde bekannt durch die charakteristische Guy-Fawkes-Maske, mit der sich die Aktivisten tarnen. Es steht für Spaß-Guerilla und politische Netzaktivisten ohne erkennbare Struktur, die mit Hacking-Attacken gegen die Scientology-Sekte und Internetzensur protestierten. Internetsicherheitsdienste und bald auch die gesamte Welt merkten schnell, dass Anonymous eine Bewegung war, die man sehr ernst nehmen sollte. Doch wer verbirgt sich eigentlich hinter den Masken? Inside Anonymous erzählt erstmalig die Geschichte dreier Mitglieder des harten Kerns: ihren Werdegang und ihre ganz persönliche Motivation, die sie zu überzeugten Hackern machte. Basierend auf vielen exklusiven Interviews bietet das Buch einen einzigartigen und spannenden Einblick in die Köpfe, die hinter der virtuellen Community stehen.

Das Phantom im Netz Kevin D. Mitnick 2012

Wicked Cool Shell Scripts Dave Taylor 2004 This useful book offers 101 fun shell scripts for solving common problems and personalizing the computing environment. Readers will find shell scripts to create an interactive calculator, a spell checker, a disk backup utility, a weather tracker, a web logfile analysis tool, a stock portfolio tracker, and much more. The cookbook style examples are all written in Bourne Shell (sh) syntax; the scripts will run on Linux, Mac OS X, and Unix.

Kunst, Wissenschaft, Natur Marcus Maeder 2017-04-30 Künste und Wissenschaften sind sich näher gekommen - besonders in ihrer Verwendung von Medientechnologien und im Einsatz von ästhetischen Praktiken. Doch wissenschaftliche Erkenntnisse sehen sich nicht nur in ihrer Vermittlung mit ästhetischen Fragen konfrontiert, sondern bereits in der Erforschung eines Gegenstands. Die Künste ihrerseits haben sich in jüngeren Disziplinen wie der Bio- oder Eco-Art auf die Naturwissenschaften zu bewegt. Die Beiträger_innen des Bandes untersuchen die erkenntnistheoretischen und ästhetischen Bedingungen, Möglichkeiten und Probleme, die sich zeigen, wenn Kunst und Wissenschaft in Kooperation treten und neue Wahrnehmungsformen der Natur schaffen. Mit Beiträgen von Marcus Maeder, Jeanine Reutemann, Hannes Rickli, Andreas Rigling und Yvonne Volkart.

Gray Hat Hacking the Ethical Hacker's Ça?atay ?anl? Why study programming? Ethical gray hat hackers should study programming and learn as much about the subject as possible in order to find vulnerabilities in programs and get them fixed before unethical hackers take advantage of them. It is very much a foot race: if the vulnerability exists, who will find it first? The purpose of this chapter is to give you the survival skills necessary to understand upcoming chapters and later find the holes in software before the black hats do. In this chapter, we cover the following topics: • C programming language • Computer memory • Intel processors • Assembly language basics • Debugging with gdb • Python survival skills

Gray Hat Python Justin Seitz 2009-04-15 Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

Die Kunst der Täuschung Kevin D. Mitnick 2012-07-10 Mitnick führt den Leser in die Denk- und Handlungsweise des Social Engineering ein, beschreibt konkrete Betrugsszenarien und zeigt eindrucksvoll die dramatischen Konsequenzen, die sich daraus ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers als auch des Opfers ein und erklärt damit sehr eindrucksvoll, wieso die Täuschung so erfolgreich war - und wie man sich effektiv dagegen schützen kann.