Blue Team Field Manual Btfm Rtfm English Edition Pdf

KENDRICK AVA

Narren des Zufalls MITP-Verlags GmbH & Co. KG
DAS INTERNET IST NICHT SICHER – FÜR KEINEN VON UNS Der weltweit bekannte IT-Sicherheitsexperte Bruce Schneier deckt die eklatanten Sicherheitslücken unserer hypervernetzten Welt auf. Identitäts- und Datendiebstahl sind dabei noch das geringste Risiko. Hacker können sogar die Kontrolle über Ihr Auto, Ihre Alarmanlage oder das nationale Stromnetz übernehmen, solange das Internet of Things nicht sicherer wird. Bruce Schneier zeigt in diesem Buch anhand beunruhigender und zugleich aufschlussreicher Fallbeispiele, wie leicht es für Hacker ist, Sicherheitslücken in Software und Protokollen auszunutzen und nahezu jedes technische Gerät unseres Alltags zu kompromittieren. Die Risiken sind unüberschaubar und können katastrophale Ausmaße annehmen. Dennoch haben Unternehmen und Regierungen bisher scheinbar kein großes Interesse daran, die IT-Sicherheit zu verbessern. Bruce Schneier beleuchtet ausführlich, wie die aktuellen Sicherheitsmängel entstanden sind und welche enormen Auswirkungen sie in Zukunft auf unser tägliches Leben haben könnten. Er fordert Regierungen mit konkreten Handlungsvorschlägen auf, das Internet of Things zukünftig verantwortungsvoll zu regulieren, und macht deutlich, was getan werden muss, um die Sicherheitslücken zu schließen. Stimmen zum Buch: »Schneiers Buch zeigt ernüchternd und aufschlussreich, wie es zu den Sicherheitsmängeln kommen konnte, die durch die zunehmende Ausbreitung des Internets auf alle Lebensbereiche entstanden sind, und was man dagegen tun sollte (und wahrscheinlich nicht tun wird).« – NATURE »Schneier führt dem Leser eindrucksvoll die massiven Hackerangriffe der Vergangenheit vor Augen – und welche er noch kommen sieht. […] Er stellt detaillierte Lösungsansätze vor, die für Politiker auf der ganzen Welt Pflichtlektüre sein sollten.« – FINANCIAL TIMES

Die Xbox hacken. Emerald Group Publishing
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.

Btfm dpunkt.verlag
The non-technical handbook for cyber security risk management Solving Cyber Risk distills a decade of research into a practical framework for cyber security. Blending statistical data and cost information with research into the culture, psychology, and business models of the hacker community, this book provides business executives, policy-makers, and individuals with a deeper understanding of existing future threats, and an action plan for safeguarding their organizations. Key Risk Indicators reveal vulnerabilities based on organization type, IT infrastructure and existing security measures, while expert discussion from leading cyber risk specialists details practical, real-world methods of risk reduction and mitigation. By the nature of the business, your organization’s customer database is packed with highly sensitive information that is essentially hacker-bait, and even a minor flaw in security protocol could spell disaster. This book takes you deep into the cyber threat landscape to show you how to keep your data secure. Understand who is carrying out cyber-attacks, and why Identify your organization’s risk of attack and vulnerability to damage Learn the most

cost-effective risk reduction measures Adopt a new cyber risk assessment and quantification framework based on techniques used by the insurance industry By applying risk management principles to cyber security, non-technical leadership gains a greater understanding of the types of threat, level of threat, and level of investment needed to fortify the organization against attack. Just because you have not been hit does not mean your data is safe, and hackers rely on their targets' complacence to help maximize their haul. Solving Cyber Risk gives you a concrete action plan for implementing top-notch preventative measures before you're forced to implement damage control.

Die Kunst des Human Hacking: Social Engineering-Deutsche Ausgabe John Wiley & Sons

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

Operation Excalibur DVA

"Fast 500.000 verkaufte Exemplare in drei Tagen - die Enthüllung von Bushs ehemaligem Terrorberater Richard Clarke schlägt alle Rekorde" (SPIEGEL ONLINE) Binnen weniger Tage wurde "Against All Enemies" zu einem hochbrisanten Politikum, über das die Medien weltweit berichteten. Was macht die Schlagkraft dieses Buches aus? "Die Bush-Administration hat die Gelegenheit verpasst, Al Qaida zu zerschlagen", schreibt Richard A. Clarke. Sie habe alle Warnungen vor Al Qaida ignoriert, in einem unnötigen Krieg gegen Irak wertvolle Zeit verloren und dem Terrorismus Gelegenheit gegeben, sich neu zu organisieren. Wie kein anderer ist Clarke berechtigt, ein solches Urteil zu fällen. Zwei Jahrzehnte seines Lebens hat er dem Kampf gegen den Terrorismus gewidmet. Er war unter Clinton und Bush Cheforganisator der amerikanischen Anti-Terror-Politik und leitete in den entscheidenden Stunden nach den Anschlägenvom 11. September den Krisenstab im Weißen Haus. Sein Bericht, der sich auf die Entwicklungen vom ersten Golfkrieg bis zu "Bushs Vietnam" im Irak konzentriert, liest sich wie ein autobiografischer Thriller.

Raspberry Pi OS System Administration with systemd and Python Pragma LLC

Seit mehr als zweitausend Jahren hat man die Worte eines heiligen Textes missverstanden. Fast alle, die sie gelesen haben, haben sie verdreht und mit einem Geheimnis umgeben. Nur ganz wenige Menschen haben im Lauf der Zeit begriffen, dass diese Worte ein Rätsel sind – ein Rätsel, das von uns gelöst werden will. Wenn Sie einmal seinen Schleier gelüftet haben, wird Ihnen die ganze Welt neu erscheinen. In THE MAGIC enthüllt Rhonda Byrne dieses geheime Wissen der ganzen Welt, und es wird auch Ihr Leben verändern! Mehr noch: Auf einer 28-tägigen Reise zeigt sie Ihnen, wie Sie es in Ihrem Alltag anwenden können. Es spielt keine Rolle, wer Sie sind; es spielt keine Rolle, wo Sie leben und was Sie gerade tun: THE MAGIC wird Ihr Leben vollkommen verändern!

Against All Enemies John Wiley & Sons

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

Verblendung dpunkt.verlag

Der Zufall ist des Glückes Schmied. Glück oder Zufall sind viel bestimmender in unserem Leben, als wir denken. Wir neigen dazu, unser Glück auf unsere eigenen Fähigkeiten zurückzuführen, den Zufall halten wir für unsere Bestimmung. Nassim Nicholas Taleb, renommierter Statistiker und Erfolgsautor des Bestsellers »Der schwarze Schwan«, entlarvt unsere menschliche Schwäche, dort Zusammenhänge zu suchen, wo keine sind.

Kuckucksei John Wiley & Sons

Blue Team Field Manual (BTFM) is a Cyber Security Incident Response Guide that aligns with the NIST Cybersecurity Framework consisting of the five core functions of Identify, Protect, Detect, Respond, and Recover by providing the tactical steps to follow and commands to use when preparing for, working through and recovering from a Cyber Security Incident.

Wie Demokratien sterben Droemer eBook

»Das wichtigste Buch der Trump-Ära« The Economist Ausgezeichnet mit dem NDR Kultur Sachbuchpreis als bestes Sachbuch des Jahres Demokratien sterben mit einem Knall oder mit einem Wimmern. Der Knall, also das oft gewaltsame Ende einer Demokratie durch einen Putsch, einen Krieg oder eine Revolution, ist spektakulärer. Doch das Dahinsiechen einer Demokratie, das Sterben mit einem Wimmern, ist alltäglicher – und gefährlicher, weil die Bürger meist erst aufwachen, wenn es zu spät ist. In ihrem mehrfach preisgekrönten Bestseller zeigen die beiden Politologen Steven Levitsky und Daniel Ziblatt, woran wir erkennen, dass demokratische Institutionen und Prozesse ausgehöhlt werden. Und sie sagen, wie wir diese Entwicklung stoppen können. Denn mit gezielter Gegenwehr lässt sich die Demokratie retten – auch vom Sterbebett.

Mr. Robot: Red Wheelbarrow Reclam Verlag

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.

Die schöne Cassandra. Sämtliche Jugendwerke BTFM

Bereits in seinen ersten Artikeln über die NSA-Affäre brachte Glenn Greenwald das ganze Ausmaß der Massenüberwachung im digitalen Zeitalter ans Licht. Seine Berichterstattung, für die er mit dem Pulitzer-Preis ausgezeichnet wurde, löste international ein politisches Erdbeben aus. In seinem Buch deckt Greenwald anhand einer Fülle von brisanten Geheimdokumenten aus dem Archiv des Whistleblowers Edward Snowden die illegalen Praktiken der amerikanischen Geheimdienste auf. Alles und jeder wird ausgespäht, die Bevölkerung steht unter Kollektivverdacht. Meinungsfreiheit wird im Namen der Sicherheit unterdrückt, und es gibt keine Privatsphäre mehr – nirgends.

CRC Press

Richard A. Clarke, Amerikas Sicherheitsexperte Nummer eins warnt: Das World Wide Web ist nicht nur ein Segen, sondern auch eine Quelle neuer Gefahren, gegen die effektive Schutzmassnahmen ergriffen werden müssen..

Das Phantom im Netz Hüthig Jehle Rehm

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!

Wabi-sabi für Künstler, Architekten und Designer Createspace Independent Publishing Platform

Was kann die neue PowerShell auf den verschiedenen Betriebssystemen? Was kann sie nicht? Dieses Buch bietet eine praxisorientierte Einführung in die PowerShell-Welt mit vielen Beispielen. Lernen Sie wichtige Cmdlets, die Arbeit mit Objekten und den Gebrauch von Funktionen, Skripten und Modulen kennen. Für Umsteiger sind besonders die Unterschiede zur Windows PowerShell interessant. Grundlegende Kenntnisse im Umgang mit Windows, Linux oder macOS sind zum Verständnis des Buchs völlig ausreichend.

PowerShell Core für Dummies Knaur MensSana eBook

Der Standard-Leitfaden – komplett aktualisiert auf Windows 10 und Windows Server 2016 Tauchen Sie in die Architektur und die inneren Mechanismen von Windows ein und lernen Sie die Kernkomponenten kennen, die hinter den Kulissen arbeiten. Dieser klassische Leitfaden wurde von einem Expertenteam für die inneren Mechanismen von Windows verfasst und vollständig auf Windows 10 und Windows Server 2016 aktualisiert. Dieses Buch gibt Entwicklern und IT-Profis entscheidende Insiderinformationen über die Funktionsweise von Windows. Durch praktische Experimente können Sie das interne Verhalten selbst erfahren und nützliche Kenntnisse zur Verbesserung des Designs Ihrer Anwendungen, zur Steigerung der Leistung, für Debugging und Support gewinnen. In diesem Buch lernen Sie: Wie die Systemarchitektur von Windows aufgebaut ist und wie ihre wichtigsten Elemente aussehen, insbesondere Prozesse und Threads Wie Prozesse Ressourcen und Threads verwalten Wie Windows virtuellen und physischen Arbeitsspeicher verwaltet Wie es in den Tiefen des E/A-Systems von Windows aussieht, wie Gerätetreiber funktionieren und wie sie mit dem Rest des Systems zusammenwirken Wie das Sicherheitsmodell von Windows Zugriff, Überwachung und Autorisierung handhabt und welche neuen Mechanismen es in Windows 10 und Windows Server 2016 gibt

(K)ein Gespür für Zahlen McGraw Hill Professional

The Cybersecurity Workforce of Tomorrow discusses the current requirements of the cybersecurity worker and analyses the ways in which these roles may change in the future as attacks from hackers, criminals and enemy states become increasingly sophisticated.

Windows Internals Redline Wirtschaft

Selbst Liebhaber ihrer sechs Romane wissen häufig nicht, dass Jane Austen schon zwischen ihrem elften und siebzehnten Lebensjahr eine ganze Reihe kürzerer fiktionaler Texte schrieb. Diese blieben lange im Besitz der Familie, die es nicht für angebracht hielt, "diesen Werdegang der Öffentlichkeit zu enthüllen". Janes Jugendwerke wurden deshalb zum allergrößten Teil erst im 20. Jahrhundert zugänglich. Es sind Texte von überbordender Phantasie, einem frechen Humor, einer unbändigen Lust, zu provozieren, die Ursula und Christian Grawe erstmals vollständig ins Deutsche übersetzt haben.

PTFM MITP-Verlags GmbH & Co. KG

Red teams can show flaws that exist in your network before they are compromised by malicious actors and blue teams traditionally assess current security measures and identify security flaws. The teams can provide valuable feedback to each other, but this is often overlooked, enter the purple team. The purple team allows for the integration of red team tactics and blue team security measures. The purple team field manual is a manual for all security professionals and integrates red and blue team methodologies.

Solving Cyber Risk MITP-Verlags GmbH & Co. KG

Tribal Knowledge from the Best in Cybersecurity Leadership The Tribe of Hackers series continues, sharing what CISSPs, CISOs, and other security leaders need to know to build solid cybersecurity teams and keep organizations secure. Dozens of experts and influential security specialists reveal their best strategies for building, leading, and managing information security within organizations. Tribe of Hackers Security Leaders follows the same bestselling format as the original Tribe of Hackers, but with a detailed focus on how information security leaders impact organizational security.

Information security is becoming more important and more valuable all the time. Security breaches can be costly, even shutting businessesand governments down, so security leadership is a high-stakes game. Leading teams of hackers is not always easy, but the future of your organization may depend on it. In this book, the world’s top security experts answer the questions that Chief Information Security Officers and other security leaders are asking, including: What’s the most important decision you’ve made or action you’ve taken to enable a business risk? How do you lead your team to execute and get results? Do you have a workforce philosophy or unique approach to talent acquisition? Have you created a cohesive strategy for your information security program or business unit? Anyone in or aspiring to an information security leadership role, whether at a team level or organization-wide, needs to read this book. Tribe of Hackers Security Leaders has the real-world advice and practical guidance you need to advance your cybersecurity leadership career.