The Social Engineers Playbook A Practical Guide To Pretexting

The missing manual on how to apply Lean Startup to build products that customers love The Lean Product Playbook is a practical guide to building products that customers love. Whether you work at a startup or a large, established company, we all know that building great products is hard. Most new products fail. This book helps improve your chances of building successful products through clear, step-by-step guidance and advice. The Lean Startup movement has contributed new and valuable ideas about product development and has generated lots of excitement. However, many companies have yet to successfully adopt Lean thinking. Despite their enthusiasm and familiarity with the high-level concepts, many teams run into challenges trying to adopt Lean because they feel like they lack specific guidance on what exactly they should be doing. If you are interested in Lean Startup principles and want to apply them to develop winning products, this book is for you. This book describes the Lean Product Process: a repeatable, easy-to-follow methodology for iterating your way to product-market fit. It walks you through how to: Determine your target customers Identify underserved customer needs Create a winning product strategy Decide on your Minimum Viable Product (MVP) Design your MVP prototype Test your MVP with customers Iterate rapidly to achieve product-market fit This book was written by entrepreneur and Lean product expert Dan Olsen whose experience spans product management, UX design, coding, analytics, and marketing across a variety of products. As a hands-on consultant, he refined and applied the advice in this book as he helped many companies improve their product process and build great products. His clients include Facebook, Box, Hightail, Epocrates, and Medallia. Entrepreneurs, executives, product managers, designers, developers, marketers, analysts and anyone who is passionate about building great products will find The Lean Product Playbook an indispensable, hands-on resource.

This how-to resource provides leaders with a concrete framework for a strategic improvement plan, helping educators link the "principles" to "processes" of planning. Packed with key takeaways and additional resources, this book provides the concrete tools to design a strong strategy for improvement and enables educational leaders to think constructively about why we plan, what an effective strategic plan should contain, and how to create meaningful dialogue to support plan development, implementation, and monitoring for continuous improvement. The Strategy Playbook for Educational Leaders provides superintendents, central office staff, principals, and teacher leaders with the opportunity to reframe the process of their strategic planning and breathe new life into the activity.

The real story behind the Tavistock Institute and its network, from a popular conspiracy expert The Tavistock Institute, in Sussex, England, describes itself as a nonprofit charity that applies social science to contemporary issues and problems. But this book posits that it is the world's center for mass brainwashing and social engineering activities. It grew from a somewhat crude beginning at Wellington House into a sophisticated organization that was to shape the destiny of the entire planet, and in the process, change the paradigm of modern society. In this eye-opening work, both the Tavistock network and the methods of brainwashing and psychological warfare are uncovered. With connections to U.S. research institutes, think tanks, and the drug industry, the Tavistock has a large reach, and Tavistock Institute attempts to show that the conspiracy is real, who is behind it, what its final long term objectives are, and how we the people can stop them.

Why do so many sports teams have losing records, year after year? Why do others win big, but only every 20 or 30 years? And why is it that so few teams enjoy sustained, continual success? This book gives the answer. Providing a blueprint or "playbook" for success in sports at every level, it lays out a clear step-by-step plan for building a team culture that will lead to winning consistently. With each step, the book

introduces real-world tools that can be easily implemented by every sports organization and coach to achieve success, including team charters, individual athlete plans, player accountability systems, and team communication strategies. It offers expert advice and practical guidance on key areas, such as aligning individuals with a clear team plan, resolving conflicts proactively, and learning from every game and every season to develop a smarter and more consistent culture of success. The Sports Playbook: Building Teams that Outperform, Year after Year will help every team fulfil its true potential through leadership, focus, and performance. It is essential reading for coaches, sport management professionals, and leaders of every kind of team, inside and outside of sports.

Back for the third season, The Hacker Playbook 3 (THP3) takes your offensive game to the pro tier. With a combination of new strategies, attacks, exploits, tips and tricks, you will be able to put yourself in the center of the action toward victory. The main purpose of this book is to answer questions as to why things are still broken. For instance, with all the different security products, secure code reviews, defense in depth, and penetration testing requirements, how are we still seeing massive security breaches happening to major corporations and governments? The real question we need to ask ourselves is, are all the safeguards we are putting in place working? This is what The Hacker Playbook 3 - Red Team Edition is all about. By now, we are all familiar with penetration testing, but what exactly is a Red Team? Red Teams simulate real-world, advanced attacks to test how well your organization's defensive teams respond if you were breached. They find the answers to questions like: Do your incident response teams have the right tools, skill sets, and people to detect and mitigate these attacks? How long would it take them to perform these tasks and is it adequate? This is where you, as a Red Teamer, come in to accurately test and validate the overall security program. THP3 will take your offensive hacking skills, thought processes, and attack paths to the next level. This book focuses on real-world campaigns and attacks, exposing you to different initial entry points, exploitation, custom malware, persistence, and lateral movement--all without getting caught! This heavily lab-based book will include multiple Virtual Machines, testing environments, and custom THP tools. So grab your helmet and let's go break things! For more information, visit http: //thehackerplaybook.com/about/.

Today, software engineers need to know not only how to program effectively but also how to develop proper engineering practices to make their codebase sustainable and healthy. This book emphasizes this difference between programming and software engineering. How can software engineers manage a living codebase that evolves and responds to changing requirements and demands over the length of its life? Based on their experience at Google, software engineers Titus Winters and Hyrum Wright, along with technical writer Tom Manshreck, present a candid and insightful look at how some of the world’s leading practitioners construct and maintain software. This book covers Google’s unique engineering culture, processes, and tools and how these aspects contribute to the effectiveness of an engineering organization. You’ll explore three fundamental principles that software organizations should keep in mind when designing, architecting, writing, and maintaining code: How time affects the sustainability of software and how to make your code resilient over time How scale affects the viability of software practices within an engineering organization What trade-offs a typical engineer needs to make when evaluating design and development decisions

This book will equip you with a holistic understanding of 'social engineering'. It will help you to avoid and combat social engineering attacks by giving you a detailed insight into how a social engineer operates. The book covers topics from baiting, phishing, and spear phishing, to pretexting and scareware.

Johnny Long's last book sold 12,000 units worldwide. Kevin Mitnick's last book sold 40,000 units in North America. As the cliché goes,

information is power. In this age of technology, an increasing majority of the world's information is stored electronically. It makes sense then that we rely on high-tech electronic protection systems to guard that information. As professional hackers, Johnny Long and Kevin Mitnick get paid to uncover weaknesses in those systems and exploit them. Whether breaking into buildings or slipping past industrial-grade firewalls, their goal has always been the same: extract the information using any means necessary. After hundreds of jobs, they have discovered the secrets to bypassing every conceivable high-tech security system. This book reveals those secrets; as the title suggests, it has nothing to do with high technology. • Dumpster Diving Be a good sport and don't read the two "D" words written in big bold letters above, and act surprised when I tell you hackers can accomplish this without relying on a single bit of technology (punny). • Tailgating Hackers and ninja both like wearing black, and they do share the ability to slip inside a building and blend with the shadows. • Shoulder Surfing If you like having a screen on your laptop so you can see what you're working on, don't read this chapter. • Physical Security Locks are serious business and lock technicians are true engineers, most backed with years of hands-on experience. But what happens when you take the age-old respected profession of the locksmith and sprinkle it with hacker ingenuity? • Social Engineering with Jack Wiles Jack has trained hundreds of federal agents, corporate attorneys, CEOs and internal auditors on computer crime and security-related topics. His unforgettable presentations are filled with three decades of personal "war stories" from the trenches of Information Security and Physical Security. • Google Hacking A hacker doesn't even need his own computer to do the necessary research. If he can make it to a public library, Kinko's or Internet cafe, he can use Google to process all that data into something useful. • P2P Hacking Let's assume a guy has no budget, no commercial hacking software, no support from organized crime and no fancy gear. With all those restrictions, is this guy still a threat to you? Have a look at this chapter and judge for yourself. • People Watching Skilled people watchers can learn a whole lot in just a few quick glances. In this chapter we'll take a look at a few examples of the types of things that draws a no-tech hacker's eye. • Kiosks What happens when a kiosk is more than a kiosk? What happens when the kiosk holds airline passenger information? What if the kiosk holds confidential patient information? What if the kiosk holds cash? • Vehicle Surveillance Most people don't realize that some of the most thrilling vehicular espionage happens when the cars aren't moving at all!

Ian Mann's Hacking the Human highlights the main sources of risk from social engineering and draws on psychological models to explain the basis for human vulnerabilities. Offering more than a simple checklist to follow, the book provides a rich mix of examples, applied research and practical solutions for security and IT professionals that enable you to create and develop a security solution that is most appropriate for your organization.

A powerful and effective Lean tool, 5S can help prevent company failure and launch an organization into world-class operational excellence. Until now, however, there has been a need for a book with detailed step-by-step guidelines on how to properly implement 5S (Sort, Set in Order, Scrub, Standardize, Sustain) and the visual workplace. Complete with color images, The 5S Playbook: A Step-by-Step Guideline for the Lean Practitioner fills this need. This new book in The LEAN Playbook Series is your guide to proper 5S and visual workplace implementation. It is ideal for Lean practitioners and facilitators looking for a training tool and a guideline that can be used in the work area while improvements are being made. Like a football coach, you can use this playbook for quick reference to convey what's needed to facilitate effective 5S kaizen events. If for some reason you forget a "play" during the 5S implementation, you can easily reference the playbook. You can follow page by page and use the playbook to facilitate a 5S implementation, or you can go directly to certain topics and use it to help you implement that particular "play." The playbook includes color images from actual 5S implementations. In addition to the

images, a combination of short paragraphs and bulleted descriptions walk you through each step of an effective 5S implementation. Looking for supplemental information or Lean coaching from Chris Ortiz? Go to www.leanplaybooks.com to receive ongoing support and advice on how to use The LEAN Playbook Series for training and implementation.

The first book to reveal and dissect the technical aspect of many social engineering maneuvers From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Kevin Mitnick—one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.

Nearly every aspect of daily life in the Mediterranean world and Europe during the florescence of the Greek and Roman cultures is relevant to the topics of engineering and technology. This volume highlights both the accomplishments of the ancient societies and the remaining research problems, and stimulates further progress in the history of ancient technology. The subject matter of the book is the technological framework of the Greek and Roman cultures from ca. 800 B.C. through ca. A.D. 500 in the circum-Mediterranean world and Northern Europe. Each chapter discusses a technology or family of technologies from an analytical rather than descriptive point of view, providing a critical summation of our present knowledge of the Greek and Roman accomplishments in the technology concerned and the evolution of their technical capabilities over the chronological period. Each presentation reviews the issues and recent contributions, and defines the capacities and accomplishments of the technology in the context of the society that used it, the available "technological shelf," and the resources consumed. These studies introduce and synthesize the results of excavation or specialized studies. The chapters are organized in sections progressing from sources (written and representational) to primary (e.g., mining, metallurgy, agriculture) and secondary (e.g., woodworking, glass production, food preparation, textile production and leather-working) production, to technologies of social organization and interaction (e.g., roads, bridges, ships, harbors, warfare and fortification), and finally to studies of general social issues (e.g., writing, timekeeping, measurement, scientific instruments, attitudes toward technology and innovation) and the relevance of ethnographic methods to the study of classical technology. The unrivalled breadth and depth of this volume make it the definitive reference work for students and academics across the spectrum of classical studies.

The #1 international best seller In Lean In, Sheryl Sandberg reignited the conversation around women in the workplace. Sandberg is chief operating officer of Facebook and coauthor of Option B with Adam Grant. In 2010, she gave an electrifying TED talk in which she described how women unintentionally hold themselves back in their careers. Her talk, which has been viewed more than six million times, encouraged women to “sit at the table,” seek challenges, take risks, and pursue their goals with gusto. Lean In continues that conversation, combining personal anecdotes, hard data, and compelling research to change the conversation from what women can’t do to what they can. Sandberg

provides practical advice on negotiation techniques, mentorship, and building a satisfying career. She describes specific steps women can take to combine professional achievement with personal fulfillment, and demonstrates how men can benefit by supporting women both in the workplace and at home. Written with humor and wisdom, Lean In is a revelatory, inspiring call to action and a blueprint for individual growth that will empower women around the world to achieve their full potential.

Despite the wide acceptance of Lean approaches and customer-development strategies, many product teams still have difficulty putting these principles into meaningful action. That's where The Customer-Driven Playbook comes in. This practical guide provides a complete end-to-end process that will help you understand customers, identify their problems, conceptualize new ideas, and create fantastic products they'll love. To build successful products, you need to continually test your assumptions about your customers and the products you build. This book shows team leads, researchers, designers, and managers how to use the Hypothesis Progression Framework (HPF) to formulate, experiment with, and make sense of critical customer and product assumptions at every stage. With helpful tips, real-world examples, and complete guides, you'll quickly learn how to turn Lean theory into action. Collect and formulate your assumptions into hypotheses that can be tested to unlock meaningful insights Conduct experiments to create a continual cadence of learning Derive patterns and meaning from the feedback you've collected from customers Improve your confidence when making strategic business and product decisions Track the progression of your assumptions, hypotheses, early ideas, concepts, and product features with step-by-step playbooks Improve customer satisfaction by creating a consistent feedback loop

This book is not about selling products -- it is about selling yourself, your ideas, and your services. This book explains an innovative dialogue sales process, and the relationship sales principles that underpin it. In every sales situation, there is both a seller and a buyer and, at different times, either the buyer or the seller may take the lead. The dance they perform may or may not lead to a deal, but it will leave them knowing a little more about each other's strengths and weaknesses. These two dancers are "connected" and follow the same steps -- The five steps they follow are to plan, connect, dialogue, record, and follow up. The five steps are the basis of the dialogue process. In addition, this book provides easy-to-follow guidance for three groups of people: 1. Professionals wanting to sell their services and improve their business development; 2. Thought leaders, change agents, innovators, entrepreneurs, senior public servants, and advocates wanting to sell their ideas to others; 3. Mid-career job seekers and recent graduates aiming to sell themselves into a dream job role either full or part-time.

A global security expert draws on psychological insights to help you master the art of social engineering—human hacking. Make friends, influence people, and leave them feeling better for having met you by being more empathetic, generous, and kind. Eroding social conventions, technology, and rapid economic change are making human beings more stressed and socially awkward and isolated than ever. We live in our own bubbles, reluctant to connect, and feeling increasingly powerless, insecure, and apprehensive when communicating with others. A pioneer in the field of social engineering and a master hacker, Christopher Hadnagy specializes in understanding how malicious attackers exploit principles of human communication to access information and resources through manipulation and deceit. Now, he shows you how to use social engineering as a force for good—to help you regain your confidence and control. Human Hacking provides tools that will help you establish rapport with strangers, use body language and verbal cues to your advantage, steer conversations and influence other's decisions, and protect yourself from manipulators. Ultimately, you'll become far more self-aware about how you're presenting yourself—and able to use it to improve your life. Hadnagy includes lessons and interactive "missions"—exercises spread throughout the book to help you learn the skills, practice them, and master them. With Human Hacking, you'll soon be winning friends, influencing people, and achieving your

goals.

An essential anti-phishing desk reference for anyone with anemail address Phishing Dark Waters addresses the growing and continuingscourge of phishing emails, and provides actionable defensivetechniques and tools to help you steer clear of malicious emails.Phishing is analyzed from the viewpoint of human decision-makingand the impact of deliberate influence and manipulation on therecipient. With expert guidance, this book provides insight intothe financial, corporate espionage, nation state, and identitytheft goals of the attackers, and teaches you how to spot a spoofede-mail or cloned website. Included are detailed examples of highprofile breaches at Target, RSA, Coca Cola, and the AP, as well asan examination of sample scams including the Nigerian 419,financial themes, and post high-profile event attacks. Learn how toprotect yourself and your organization using anti-phishing tools,and how to create your own phish to use as part of a securityawareness program. Phishing is a social engineering technique through email thatdeceives users into taking an action that is not in their bestinterest, but usually with the goal of disclosing information orinstalling malware on the victim's computer. Phishing DarkWaters explains the phishing process and techniques, and thedefenses available to keep scammers at bay. Learn what a phish is, and the deceptive ways they've beenused Understand decision-making, and the sneaky ways phishers reelyou in Recognize different types of phish, and know what to do whenyou catch one Use phishing as part of your security awareness program forheightened protection Attempts to deal with the growing number of phishing incidentsinclude legislation, user training, public awareness, and technicalsecurity, but phishing still exploits the natural way humansrespond to certain situations. Phishing Dark Waters is anindispensible guide to recognizing and blocking the phish, keepingyou, your organization, and your finances safe.

The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception Are You Ready To Learn How To Configure & Operate Cisco Equipment? If So You've Come To The Right Place - Regardless Of How Little Experience You May Have! If you're interested in social engineering and security then you're going to want (or need!) to know and understand the way of the social engineer. There's a ton of other guides out there that aren't clear and concise, and in my opinion use far too much jargon. My job is to teach you in simple, easy to follow terms how to understand social engineering. Here's A Preview Of What This Social Engineering Book Contains... What Is Social Engineering? Basic Psychological Tactics Social Engineering Tools Pickup Lines Of Social Engineers How To Prevent And Mitigate Social Engineering Attacks And Much, Much More! Order Your Copy Now And Learn All About Social Engineering!

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test,

Metasploit: The Penetration Tester's Guide will take you there and beyond.

Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker's repertoire-why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the "system" in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer's bag of tricks. Examine the most common social engineering tricks used to gain access Discover which popular techniques generally don't work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer's playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.

A manual for the very first physical red team operation methodology. This book teaches how to execute every stage of a physical red team operation fromreconnaissance, to team mobilization, to offensive strike, and exfiltration. Forthe first time in the physical red teaming industry, a consistent, repeatable, andcomprehensive step-by-step introduction to the REDTEAMOPSEC methodology -created and refined by Jeremiah Talamantes of RedTeam Security - subject ofthe viral documentary titled, "Hacking the Grid."

This book is for cybersecurity leaders across all industries and organizations. It is intended to bridge the gap between the data center and the board room. This book examines the multitude of communication challenges that CISOs are faced with every day and provides practical tools to identify your audience, tailor your message and master the art of communicating. Poor communication is one of the top reasons that CISOs fail in their roles. By taking the step to work on your communication and soft skills (the two go hand-in-hand), you will hopefully never join their ranks. This is not a “communication theory” book. It provides just enough practical skills and techniques for security leaders to get the job done. Learn fundamental communication skills and how to apply them to day-to-day challenges like communicating with your peers, your team, business leaders and the board of directors. Learn how to produce meaningful metrics and communicate before, during and after an incident. Regardless of your role in Tech, you will find something of value somewhere along the way in this book.

Learn to identify the social engineer by non-verbal behavior Unmasking the Social Engineer: The Human Element of Security focuses on combining the science of understanding non-verbal communications with the knowledge of how social engineers, scam artists and con men use these skills to build feelings of trust and rapport in their targets. The author helps readers understand how to identify and detect social engineers and scammers by analyzing their non-verbal behavior. Unmasking the Social Engineer shows how attacks work, explains nonverbal communications, and demonstrates with visuals the connection of non-verbal behavior to social engineering and scamming.

Clearly combines both the practical and technical aspects of social engineering security Reveals the various dirty tricks that scammers use Pinpoints what to look for on the nonverbal side to detect the social engineer Sharing proven scientific methodology for reading, understanding, and deciphering non-verbal communications, Unmasking the Social Engineer arms readers with the knowledge needed to help protect their organizations.

This book analyzes of the use of social engineering as a tool to hack random systems and target specific systems in several dimensions of society. It shows how social engineering techniques are employed well beyond what hackers do to penetrate computer systems. And it explains how organizations and individuals can socially engineer their culture to help minimize the impact of the activities of those who lie, cheat, deceive, and defraud. After reading this book, you'll be able to analyze how organizations work and the need for security to maintain operations and sustainability, and be able to identify, respond to and counter socially engineered threats to security.

Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker's repertoire—why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the "system" in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer's bag of tricks. Examine the most common social engineering tricks used to gain access Discover which popular techniques generally don't work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer's playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.

A companywide approach to improving the effectiveness and longevity of equipment and machines, Total Productive Maintenance (TPM) is a critical component of production line success. The need for a step-by-step guidelines on how to achieve TPM has been filled with the publication of The TPM Playbook: A Step-by-Step Guideline for the Lean Practitione

If you create, manage, operate, or configure systems running in the cloud, you're a cloud engineer--even if you work as a system administrator, software developer, data scientist, or site reliability engineer. With this book, professionals from around the world

provide valuable insight into today's cloud engineering role. These concise articles explore the entire cloud computing experience, including fundamentals, architecture, and migration. You'll delve into security and compliance, operations and reliability, and software development. And examine networking, organizational culture, and more. You're sure to find 1, 2, or 97 things that inspire you to dig deeper and expand your own career. "Three Keys to Making the Right Multicloud Decisions," Brendan O'Leary "Serverless Bad Practices," Manases Jesus Galindo Bello "Failing a Cloud Migration," Lee Atchison "Treat Your Cloud Environment as If It Were On Premises," Iyana Garry "What Is Toil, and Why Are SREs Obsessed with It?", Zachary Nickens "Lean QA: The QA Evolving in the DevOps World," Theresa Neate "How Economies of Scale Work in the Cloud," Jon Moore "The Cloud Is Not About the Cloud," Ken Corless "Data Gravity: The Importance of Data Management in the Cloud," Geoff Hughes "Even in the Cloud, the Network Is the Foundation," David Murray "Cloud Engineering Is About Culture, Not Containers," Holly Cummins

Great is no longer good enough. Beyond Great delivers a powerful new playbook of 9 core strategies to thrive in a post-COVID world where all the rules of the game are being re-written. Beyond Great answers to two fundamental questions which face business leaders today in a world shaped by daunting and disruptive technological, economic, and social change. First, what is outstanding performance in this new volatile era? Second, how do we build competitive advantage in a world with new and often uncertain rules? Supported by years of research and hands-on consulting practice, this book presents a comprehensive framework for building a high performing, resilient, adaptive, and socially responsible global company. The book begins by taking an incisive look at these disruptive forces transforming globalization, including economic nationalism; the boom in data flows and digital commerce; the rise of China; heightened public concerns about capitalism and the environment; and the emergence of borderless communities of digitally connected consumers. Distilled from the study of hundreds of companies and interviews with dozens of business leaders, the authors have distilled nine core strategies – the new winning playbook of the 21st century. Beyond Great argues that business leaders today must lead with a new kind of openness, flexibility and light-footedness, constantly layering in new strategies and operational norms atop existing ones to allow for "always-on" transformation. Leaders must master a whole new set of rules about what it takes to be "global," becoming shapeshifters adept at handling contradiction, multiplicity, and nuance. This book will show them how.

Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice

within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.

Many educators appreciate the value of interest-based learning, but struggle with the management and facilitation of individual and small-group projects in a limited space and time allocation. This easy-to-read guide: Features a step-by-step plan for managing Genius Hour, passion projects, Makerspaces, and more. Includes time-saving planning templates, checklists, and charts. Supports students' intrinsic motivation for learning, agency, voice, and problem-solving and critical thinking skills. Provides a systematic and practical approach to interest-based learning. Can be implemented and adapted by an individual teacher, department, or team. Chapters also include techniques for helping students identify their interests, frame their goals and questions, create project plans and timelines, self-assess their progress, and share their work with real-world audiences.

This book describes how to effectively implement cell manufacturing. It covers the eight Wastes of Lean and the six Lean metrics that are recommended in each implementation and a description of what cell manufacturing is and its application to improving operational processes.

Get up to speed with various penetration testing techniques and resolve security threats of varying complexity Key Features Enhance your penetration testing skills to tackle security threats Learn to gather information, find vulnerabilities, and exploit enterprise defenses Navigate secured systems with the most up-to-date version of Kali Linux (2019.1) and Metasploit (5.0.0) Book Description Sending information via the internet is not entirely private, as evidenced by the rise in hacking, malware attacks, and security threats. With the help of this book, you'll learn crucial penetration testing techniques to help you evaluate enterprise defenses. You'll start by understanding each stage of pentesting and deploying target virtual machines, including Linux and Windows. Next, the book will guide you through performing intermediate penetration testing in a controlled environment. With the help of practical use cases, you'll also be able to implement your learning in real-world scenarios. By studying everything from setting up your lab, information gathering and password attacks, through to social engineering and post exploitation, you'll be able to successfully overcome security threats. The book will even help you leverage the best tools, such as Kali Linux, Metasploit, Burp Suite, and other open source pentesting tools to perform these techniques. Toward the later chapters, you'll focus on best practices to quickly resolve security threats. By the end of this book, you'll be well versed with various penetration testing techniques so as to be able to tackle security threats effectively What you will learn Perform entry-level penetration tests by learning various concepts and techniques Understand both common and not-so-common vulnerabilities from an attacker's perspective Get familiar with intermediate attack methods that can be used in real-world scenarios Understand how vulnerabilities

are created by developers and how to fix some of them at source code level Become well versed with basic tools for ethical hacking purposes Exploit known vulnerable services with tools such as Metasploit Who this book is for If you're just getting started with penetration testing and want to explore various security domains, this book is for you. Security professionals, network engineers, and amateur ethical hackers will also find this book useful. Prior knowledge of penetration testing and ethical hacking is not necessary.

Social engineering attacks target the weakest link in an organization's security human beings. Everyone knows these attacks are effective, and everyone knows they are on the rise. Now, Social Engineering Penetration Testing gives you the practical methodology and everything you need to plan and execute a social engineering penetration test and assessment. You will gain fascinating insights into how social engineering techniques including email phishing, telephone pretexting, and physical vectors can be used to elicit information or manipulate individuals into performing actions that may aid in an attack. Using the book's easy-to-understand models and examples, you will have a much better understanding of how best to defend against these attacks. The authors of Social Engineering Penetration Testing show you hands-on techniques they have used at RandomStorm to provide clients with valuable results that make a real difference to the security of their businesses. You will learn about the differences between social engineering pen tests lasting anywhere from a few days to several months. The book shows you how to use widely available open-source tools to conduct your pen tests, then walks you through the practical steps to improve defense measures in response to test results. Understand how to plan and execute an effective social engineering assessment Learn how to configure and use the open-source tools available for the social engineer Identify parts of an assessment that will most benefit time-critical engagements Learn how to design target scenarios, create plausible attack situations, and support various attack vectors with technology Create an assessment report, then improve defense measures in response to test results

A collection of popular essays from security guru Bruce Schneier In his latest collection of essays, security expert Bruce Schneier tackles a range of cybersecurity, privacy, and real-world security issues ripped from the headlines. Essays cover the ever-expanding role of technology in national security, war, transportation, the Internet of Things, elections, and more. Throughout, he challenges the status quo with a call for leaders, voters, and consumers to make better security and privacy decisions and investments. Bruce’s writing has previously appeared in some of the world's best-known and most-respected publications, including The Atlantic, the Wall Street Journal, CNN, the New York Times, the Washington Post, Wired, and many others. And now you can enjoy his essays in one place—at your own speed and convenience. • Timely security and privacy topics • The impact of security and privacy on our world • Perfect for fans of Bruce’s blog and newsletter • Lower price than his previous essay collections The essays are written for anyone who cares about the future and implications of security and privacy for society.

As a community, aligning efforts across a community to support the safety and well-being of vulnerable and underserved individuals is extraordinarily difficult. These individuals suffer disproportionally from health issues, job loss, a lack of stable housing, high utility costs, substance abuse, and homelessness. In addition to medical care, these individuals often critically need access to community social sector organizations that provide a distinct and complementary set of services, such as housing, food services, emergency utility assistance, and employment assistance. These services are just as vital as healthcare services to these individuals’ long-term health and well-being, with data suggesting that 80–90% of health outcomes can be attributed to factors beyond direct medical intervention. This book proposes a novel

approach to the coordination of medicine and social services through the use of people, process, and technology, with the goal being to streamline coordination between medical and Community-Based Organizations and to promote true cross-sector patient and client advocacy. The book is based on the experience of Dallas, TX, which was one of the first metropolitan regions to develop a comprehensive foundation for partnership between a community's clinical and social sectors using web-based information exchange. In the 5 years since the initial launch, the authors have been able to provide seamless connection, communication, and coordination between healthcare providers and a wide array of community-based social service organizations (a/k/a Community-Based Organizations or CBOs), criminal justice entities, and various other community organizations, including non-collegiate educational systems. This practical how-to guide is the codification of transferrable lessons from successes and challenges faced when working with clinical, community, and government leaders. By reading this playbook, leaders interested in building (or expanding) connected clinical-community services will learn how to: 1) facilitate cross-sector care coordination; 2) enable community care partners to better provide targeted services to community residents; 3) reduce duplication of services across partnering organizations; and 4) help to bridge service gaps in the currently fragmented system. Implementation of services, as recommended in this book, will ultimately streamline assistance efforts, reduce repeat crises and emergency funding requests, help address disparities of care, and improve the health, safety, and well-being of the most vulnerable community residents.

JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties

An optimistic--but realistic and feasible--action plan for fighting climate change while creating new jobs and a healthier environment: electrify everything. Climate change is a planetary emergency. We have to do something now—but what? Saul Griffith has a plan. In Electrify, Griffith lays out a detailed blueprint—optimistic but feasible—for fighting climate change while creating millions of new jobs and a healthier environment. Griffith's plan can be summed up simply: electrify everything. He explains exactly what it would take to transform our infrastructure, update our grid, and adapt our households to make this possible. Billionaires may contemplate escaping our worn-out planet on a private rocket ship to Mars, but the rest of us, Griffith says, will stay and fight for the future. Griffith, an engineer and inventor, calls for grid neutrality, ensuring that households, businesses, and utilities operate as equals; we will have to rewrite regulations that were created for

a fossil-fueled world, mobilize industry as we did in World War II, and offer low-interest “climate loans.” Griffith’s plan doesn’t rely on big, not-yet-invented innovations, but on thousands of little inventions and cost reductions. We can still have our cars and our houses—but the cars will be electric and solar panels will cover our roofs. For a world trying to bounce back from a pandemic and economic crisis, there is no other project that would create as many jobs—up to twenty-five million, according to one economic analysis. Is this politically possible? We can change politics along with everything else.

"Presents guidance for communicating the value of highway system maintenance and preservation. The report includes numerous examples and models that transportation agency staff members can use to present to agency leadership, elected officials, and the public to make the case for allocating budgetary and other resources to preserve and maintain the public's investment in highway infrastructure."--Publisher's description.

The Social Engineer's Playbook is a practical guide to pretexting and a collection of social engineering pretexts for Hackers, Social Engineers and Security Analysts. Build effective social engineering plans using the techniques, tools and expert guidance in this book. Learn valuable elicitation techniques, such as: Bracketing, Artificial Ignorance, Flattery, Sounding Board and others. This book covers an introduction to tools, such as: Maltego, Social Engineer Toolkit, Dradis, Metasploit and Kali Linux among others. Crucial to any social engineering test is the information used to build it. Discover the most valuable sources of intel and how to put them to use.

The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.