Hacking Etico 101

Recognizing the pretentiousness ways to get this book **Hacking Etico 101** is additionally useful. You have remained in right site to begin getting this info. acquire the Hacking Etico 101 belong to that we give here and check out the link.

You could buy guide Hacking Etico 101 or get it as soon as feasible. You could quickly download this Hacking Etico 101 after getting deal. So, like you require the books swiftly, you can straight get it. Its appropriately unconditionally easy and therefore fats, isnt it? You have to favor to in this impression

Hacking Etico 101 - Cómo Hackear Profesionalmente en 21 días o Menos! UNESCO Publishing People can be so resistant to your ideas. Wouldn't you like to be able to slip into someone's mind and make him or her do your bidding? Since the days of crazy CIA mind control experiments, a series of highly secretive methods of subliminal mind control have been available. But they have been kept under wraps because of their power. Now you

can find them out for yourself and make your life what you want it to be by gaining control over the minds of others. Subliminal psychology is a special and top secret science that explores how to enter someone's subconscious mind. There, you can plant ideas that the person will start acting on without knowing why. Using signals, gestures, images, scents, sounds, touch, and words, you can influence someone tremendously and very stealthily. No one will know why they do the things they do under your influence. Subliminal psychology has a huge variety of uses. In this book, you will learn how to use it for seduction and settling conflict in your personal relationships. You will also use it to beat the odds in competitions. You will learn how to use it to make work better for you, and to gain dominance over others. You will learn how to apply it to parenting and relationships of all kinds. Finally, you will learn how to utilize it on yourself to bring out your best, end bad habits, and build confidence and self-esteem through positive thinking. Hack your own mind. Or hack others'. The secrets to how are all in these pages.

The Pentester BluePrint Harvard University Press

El libro est dirigido a entusiastas de la informtica que desean iniciarse en el interesante tema del hacking tico de redes inalmbricas.En l se describen de forma prctica y amena las tcnicas usadas por los hackers para explotar vulnerabilidades y penetrar las defensas de las WiFi, de la mano de la popular suite Kali Linux.Tpicos cubiertos:* Introduccin al WiFi Hacking* En qu consiste el Wardriving*

Metodologa de un WiFi Hacking* Mapeo inalmbrico* Ataques a redes y clientes WiFi* Cmo vencer el control por MAC* Ataques a los protocolos WEP, WPA, WPA2* Ataques a WPS* Creacin de rogue AP's* Ataques MITM a clientes inalmbricos y captura de datos* Engaos a clientes inalmbricos para burlar el cifrado SSL* Secuestro de sesiones a clientes inalmbricos* Mecanismos defensivos

The Art of Intrusion

Adidas Wilson Aimed towards anyone tired of spending countless hours training with weights and doing cardio and without seeing additional gains, "101 High-Intensity Workouts For Fast Results" provides a lifetime of workouts that continually increase lean muscle mass and reduce body fat using scientifically proven methods of short, high-intensity bouts of training.

Ethical Hacking 101 **John Wiley & Sons**

It's often said that success leaves clues.In Internet Business Insights, Chris Naish and Buck Flogging present interviews from 101 renowned entrepreneurial experts from a diverse range of fields. From those who can teach you to make a comfortable living with internet marketing, to a businesswoman who went from $135k of debt, to selling her company to Bill Gates.

Wireless Hacking 101 Random House

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak,

Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple II.

Ethical Hacking

Francesco Cammardella

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass

antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

CUCKOO'S EGG

"O'Reilly Media, Inc."

How to Hack Like a Ghost takes you deep inside the mind of a hacker as you carry out a fictionalized attack against a tech company, teaching cutting-edge hacking techniques along the way. Go deep into the mind of a master hacker as he breaks into a hostile, cloud-based security environment. Sparc Flow invites you to shadow him every step of the way, from recon to infiltration, as you hack a shady, data-driven political consulting firm. While the target is fictional, the corporation's vulnerabilities are based on real-life weaknesses in today's advanced cybersecurity defense systems. You'll experience all the thrills, frustrations, dead-ends, and eureka moments of his mission first-hand, while picking up practical, cutting-edge techniques for penetrating cloud technologies. There are no do-overs for hackers, so your training starts with basic OpSec procedures, using an ephemeral OS, Tor, bouncing servers, and detailed code to build an anonymous, replaceable hacking infrastructure guaranteed to avoid detection. From there, you'll examine some effective recon techniques, develop tools from scratch, and deconstruct low-level features in common systems to gain access to the target. Spark Flow's clever insights, witty reasoning, and stealth maneuvers teach you how to think on your toes and adapt his skills to your own hacking tasks. You'll learn: • How to set up and use an array of disposable machines

that can renew in a matter of seconds to change your internet footprint • How to do effective recon, like harvesting hidden domains and taking advantage of DevOps automation systems to trawl for credentials • How to look inside and gain access to AWS's storage systems • How cloud security systems like Kubernetes work, and how to hack them • Dynamic techniques for escalating privileges Packed with interesting tricks, ingenious tips, and links to external resources, this fast-paced, hands-on guide to penetrating modern cloud systems will help hackers of all stripes succeed on their next adventure.

Ediciones ENI

WIRELESS HACKING 101 – Piratage éthique des réseaux WiFi sans effort! Ce livre est dédié aux passionnés d'informatique qui cherchent à explorer le monde du piratage éthique et qui veulent se lancer dans les tests d'intrusion sur les réseaux WiFi. Vous y trouverez des informations étape par étape sur la manière d'exploiter les réseaux WiFi à l'aide d'outils inclus dans la populaire distribution Kali Linux, comme la suite aircrack-ng. Sujets traités: Introduction au piratage WiFi En quoi consiste le Wardriving Méthodologie pour un piratage WiFi Analyser les réseaux sans fil Attaquer les réseaux WiFi et ses utilisateurs Contournement du filtrage par MAC Attaques pour les protocoles WEP, WPA, WPA2 Attaques par WPS Création d'un Rogue AP Attaques MITM aux clients WiFi et capture de données Tromper les clients WiFi pour contourner le cryptage SSL Détournement de session des clients WiFi Systèmes de

défense

101 Ethical Dilemmas No Starch Press

¿Siente curiosidad sobre cómo realizan pruebas de intrusión los hackers? ¿Ha querido tomar cursos presenciales de hacking ético pero no tiene el tiempo o el dinero para hacerlo?Este libro tiene la respuesta para Usted. Con tan sólo 2 horas de dedicación diaria usted puede convertirse en hacker ético profesional!En él encontrará información paso a paso acerca de cómo actúan los hackers, cuáles son las fases que siguen, qué herramientas usan y cómo hacen para explotar vulnerabilidades en los sistemas informáticos. Aprenderá además cómo escribir un informe profesional y mucho más!El libro tiene un enfoque práctico y ameno e incluye laboratorios detallados con populares sistemas operativos como Windows y Kali Linux 2.0.Tópicos cubiertos:* El círculo del hacking* Tipos de Hacking, modalidades y servicios opcionales* Reconocimiento pasivo y activo* Google hacking, consultas WhoIs y nslookup* Footprinting con Maltego y Sam Spade* Métodos de escaneo y estados de puertos* Escaneo con NMAP* Análisis de vulnerabilidades con NeXpose y OpenVAS* Enumeración de Netbios* Mecanismos de hacking* Frameworks de explotación* Metasploit Framework (msfconsole, web y Armitage)* Ataques de claves* Ataques de malware* Ataques DoS* Hacking de Windows con Kali Linux y Metasploit* Hacking inalámbrico con Aircrack-ng* Captura de claves

con sniffers de red* Ataques MITM con Ettercap y Wireshark* Ingeniería social con el Social Engineering Toolkit (SET)* Phishing e inyección de malware con SET* Hacking de Metasploitable Linux con Armitage* Consejos para escribir un buen informe de auditoría* Certificaciones de seguridad informática y hacking relevantesSobre la autora:Karina Astudillo es una consultora de sistemas con más de 20 años de experiencia en tecnologías de información. Es experta en seguridad informática, hacker ético certificado (CEH) y tiene a su haber otras certificaciones en IT como CCNA Security, CCNA Routing & Switching, CCNA Wireless, Cisco Security, Computer Forensics US, HCSA, HCSP, Network Security, Internet Security, SCSA y VmWare VSP.En la actualidad se desenvuelve como Gerente de IT de Elixircorp, empresa consultora de seguridad informática especializada en hacking ético y computación forense.Karina es además docente de la Maestría de Seguridad Informática Aplicada (MSIA) y del Cisco Networking Academy Program (CNAP) de la Escuela Superior Politécnica del Litoral (ESPOL), en donde ha sido instructora desde 1996.

Kali Linux Revealed

Springer

The Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. No prior experience is needed. Web apps are a "path of least resistance" that can be exploited to cause the most damage to a system, with the lowest hurdles to

overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabilities. The Basics of Web Hacking provides a simple and clean explanation of how to utilize tools such as Burp Suite, sqlmap, and Zed Attack Proxy (ZAP), as well as basic network scanning tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more. Dr. Josh Pauli teaches software security at Dakota State University and has presented on this topic to the U.S. Department of Homeland Security, the NSA, BlackHat Briefings, and Defcon. He will lead you through a focused, three-part approach to Web security, including hacking the server, hacking the Web app, and hacking the Web user. With Dr. Pauli's approach, you will fully understand the what/where/why/how of the most widespread Web vulnerabilities and how easily they can be exploited with the correct tools. You will learn how to set up a safe environment to conduct these attacks, including an attacker Virtual Machine (VM) with all necessary tools and several known-vulnerable Web application VMs that are widely available and maintained for this very purpose. Once you complete the entire process, not only will you be prepared to test for the most damaging Web exploits, you will also be prepared to conduct more advanced Web hacks that mandate a strong base of knowledge. Provides a simple and clean approach to Web hacking, including hands-on examples and exercises that are designed to teach you how to hack the server, hack the Web app, and hack the Web user Covers the most significant new tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more!

Written by an author who works in the field as a penetration tester and who teaches Web security classes at Dakota State University

Penetration Testing No Starch Press

You don't need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and Game Hacking will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to: –Scan and modify memory with Cheat Engine –Explore program structure and execution flow with OllyDbg –Log processes and pinpoint useful data files with Process Monitor –Manipulate control flow through NOPing, hooking, and more –Locate and dissect common game memory structures You'll even discover the secrets behind common game bots, including: –Extrasensory perception hacks, such as wallhacks and heads-up displays –Responsive hacks, such as autohealers and combo bots –Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn't have to be. Once you understand how bots are made, you'll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with Game Hacking, and leave with a deeper understanding of both game design and computer security.

Blue Team Field Manual Springer Nature

Wireless Hacking 101 - How to hack wireless networks

easily! This book is perfect for computer enthusiasts that want to gain expertise in the interesting world of ethical hacking and that wish to start conducting wireless pentesting. Inside you will find step-by-step instructions about how to exploit WiFi networks using the tools within the known Kali Linux distro as the famous aircrack-ng suite. Topics covered: •Introduction to WiFi Hacking •What is Wardriving •WiFi Hacking Methodology •WiFi Mapping •Attacks to WiFi clients and networks •Defeating MAC control •Attacks to WEP, WPA, and WPA2 •Attacks to WPS •Creating Rogue AP's •MITM attacks to WiFi clients and data capture •Defeating WiFi clients and evading SSL encryption •Kidnapping sessions from WiFi clients •Defensive mechanisms

Major Challenges Facing Higher Education in the Arab World: Quality Assurance and Relevance

Sitepoint Pty Limited

¿Siente curiosidad sobre cómo realizan pruebas de intrusión los hackers? ¿Ha querido tomar cursos presenciales de hacking ético pero no tiene el tiempo o el dinero para hacerlo?Este libro tiene la respuesta para Usted. Con tan sólo 2 horas de dedicación diaria usted puede convertirse en hacker ético profesional!En él encontrará información paso a paso acerca de cómo actúan los hackers, cuáles son las fases que siguen, qué herramientas usan y cómo hacen para explotar vulnerabilidades en los sistemas informáticos. Aprenderá además cómo escribir un informe profesional y mucho más!El libro tiene un enfoque

práctico y ameno e incluye laboratorios detallados con populares sistemas operativos como Windows y Kali Linux (antes Backtrack).Tópicos cubiertos: El círculo del hacking Tipos de Hacking, modalidades y servicios opcionales Reconocimiento pasivo y activo Google hacking, consultas WhoIs y nslookup Footprinting con Maltego y Sam Spade Métodos de escaneo y estados de puertos Escaneo con NMAP Análisis de vulnerabilidades con NeXpose y OpenVAS Enumeración de Netbios Mecanismos de hacking Frameworks de explotación Metasploit Framework (msfconsole, web y Armitage) Ataques de claves Ataques de malware Ataques DoS Hacking de Windows con Kali Linux y Metasploit Hacking inalámbrico con Aircrack-ng Captura de claves con sniffers de red Ataques MITM con Ettercap y Wireshark Ingeniería social con el Social Engineering Toolkit (SET) Phishing e inyección de malware con SET Hacking de Metasploitable Linux con Armitage Consejos para escribir un buen informe de auditoría Certificaciones de seguridad informática y hacking relevantes

Hacking ético con herramientas Python Babelcube Inc.

How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto “we open governments” on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous.

Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l'époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d'être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d'encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L'activisme en sécurité est à la hausse. Le piratage éthique est l'utilisation non-

violence d'une technologie quelconque en soutien d'une cause politique ou autre qui est souvent ambigue d'un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivisme et la désobéissance civile en ligne.
L'hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivisme croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.

Learn Python in a Weekend Allen & Unwin

The contents in this book will provide practical hands on

implementation and demonstration guide on how you can use Kali Linux to deploy various attacks on both wired and wireless networks. If you are truly interested in becoming an Ethical Hacker or Penetration Tester, this book is for you.NOTE: If you attempt to use any of this tools on a wired or wireless network without being authorized and you disturb or damage any systems, that would be considered illegal black hat hacking. Therefore, I would like to encourage all readers to implement any tool described in this book for WHITE HAT USE ONLY!BUY THIS BOOK NOW AND GET STARTED TODAY!This book will cover: -How to Install Virtual Box & Kali Linux-Pen Testing @ Stage 1, Stage 2 and Stage 3-What Penetration Testing Standards exist-How to scan for open ports, host and network devices-Burp Suite Proxy setup and Spidering hosts-How to deploy SQL Injection with SQLmap-How to implement Dictionary Attack with Airodump-ng-How to deploy ARP Poisoning with EtterCAP-How to capture Traffic with Port Mirroring & with Xplico-How to deploy Passive Reconnaissance-How to implement MITM Attack with Ettercap & SSLstrip-How to Manipulate Packets with Scapy-How to deploy Deauthentication Attack-How to capture IPv6 Packets with Parasite6-How to deploy Evil Twin Deauthentication Attack with mdk3-How to deploy DoS Attack with MKD3-How to implement Brute Force Attack with TCP Hydra-How to deploy Armitage Hail Mary-The Metasploit Framework-How to use SET aka Social-Engineering Toolkit and more.BUY THIS BOOK NOW AND GET

STARTED TODAY!

Ethical Hacking With Kali Linux Createspace Independent Publishing Platform

This book focuses on two crucial issues that need to be addressed as a matter of urgency by universities in the Arab region, namely (a) conducting independent assessments of the quality of their teaching, research, administration, governance, and planning; and (b) determining the relevance of their teaching, research, and societal impacts. Although well-established around the world in manufacturing industries and private-sector service industries, including the research and commercialisation arms of the major universities and research institutes, it is only in recent years that quality-assurance (QA) assessments have started to be applied to most aspects education. Several Arab universities are adopting various forms of QA but some variants are little more than bureaucratic "box-ticking" exercises with minimal commitment by staff to the ultimate aim of continuing self-improvement. This book will be of interest to senior management at faculty and departmental level and above in all Arab universities specifically, and more generally in Islamic institutions of higher education. Senior management in other universities, especially in the developing world will benefit from its analyses and recommendations.

Learn Ethical Hacking from Scratch Babelcube Inc.

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to

secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact

with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts. Hacking Wireless 101 University of Ottawa Press LEARN PYTHON IN THE FASTEST AND EASIEST WAY Learn Python in a weekend offers you a learning method that will allow you to learn Python in a short period of time, specifically in a weekend!Our experience has demonstrated us that the best way to learn is to do it while having fun and with a methodology that will teach you progressively all the concepts you need to know.In the first part of the book you will find an explanation of the programming language along with an introduction to the programming environment.In the second part of the book you will find a total of 100 exercises of progressive difficulty in which, in addition to guiding you step by step, we explain all the theoretical concepts of programming that you need to know to be able to carry them out. The book contains downloadable material! INDEX 1. Introduction2.- What do I need to start?3.- Learning process4.- Python5.- Development

environment6.- Handling of messages on the screen7.- Use of basic data types8.- Control of the flow of a program9.- Loops10.- Project 111.- Functions12.- Project 213.- Basic object-oriented programming14.- Project 315.- Advanced object-oriented programming16.- Working with files17.- Exception control18.- Project 419.- Final Project20.- Annexes

Terrorism and the media Createspace Independent Publishing Platform

Hacking Etico 101 - Cómo Hackear Profesionalmente en 21 días o Menos!Createspace Independent Publishing Platform

Hacking Etico 101

Hacking Etico 101 - Cómo Hackear Profesionalmente en 21 días o Menos!

This book considers the question: to what extent does it make sense to qualify technical artefacts as moral entities? The authors' contributions trace recent proposals and topics including instrumental and non-instrumental values of artefacts, agency and artefactual agency, values in and around technologies, and the moral significance of technology. The editors' introduction explains that as 'agents' rather than simply passive instruments, technical artefacts may actively influence their users, changing the way they perceive the world, the way they act in the world and the way they interact with each other. This volume features the work of various experts from around the world, representing a variety of positions on the topic. Contributions explore the contested discourse on agency in humans and artefacts, defend the Value Neutrality Thesis by arguing that technological artefacts do not contain, have or exhibit values, or argue that moral agency involves both human and non-human elements. The book also investigates technological fields that are subject to negative moral valuations due to the harmful effects of some of their products. It includes

an analysis of some difficulties arising in Artificial Intelligence and an exploration of values in Chemistry and in Engineering. The Moral Status of Technical Artefacts is an advanced exploration of the various dimensions of the relations between technology and morality