Continue

Disclosure: Hackr.io is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Key takeaways: From basic scans to advanced exploits, the CEH exam preparation books dive into the tools and tricks used by ethical hackers. With the help of the best CEH books, you will gain a step-by-step understanding, from planning and executing tests to writing reports. CEH books stress the importance of staying up-to-date on exam trends. Depend on the best books to ensure your success in the CEH exam. Are you aspiring to become a Certified Ethical Hacker (CEH)? One of the crucial steps toward achieving this goal is selecting the right study materials. With numerous resources available, choosing the best CEH books can significantly impact your exam preparation and success. In this guide, we'll explore top-rated CEH books that provide comprehensive coverage of essential topics, effective study strategies, and practical insights to help you crack the exam and excel in the field of ethical hacking. Here are some of the top picks: CEH V11 Certified Ethical Hacker Study Guide by Ric Messier This study guide by Ric Messier covers all the essential topics you need to know for the exam, like hacking concepts, network security, and malware threats. The book focuses on what you will be tested on in the exam, including practical exercises. Moreover, the examples will help you understand concepts better and prepare for real-world cases. If you are looking forward to becoming a CEH and boosting your cybersecurity career, this beginner-level book is a great option. CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition by Matthew Walker This book covers everything you need to know for the CEH exam. This book provides comprehensive learning from the foundation of ethical hacking to cloud computing security. Ideal for intermediate-level, this book by Matt Walker begins each chapter with learning objectives, exam advice, sample test questions, and thorough explanations. Moreover, it has practice questions similar to those on the actual exam, helping you get familiar with the format and difficulty level with the most up-to-date information. Three hundred practice questions, along with chapter-based quizzes, are what make this book worth a buy! CEH Certified Ethical Hacke All-in-One Exam Guide by Matthew Walker explains ethical hacking concepts, tools, and techniques. The book is designed for the CEH exam, so you will study precisely what you need to pass. Each chapter ends with practice questions to test your knowledge and prepare you for the exam. In short, if you want to ace the CEH exam and boost your career, this intermediate-level book is a must-have! Certified Ethical Hacker (CEH) V12 312-50 Exam Guide by Dale Meredith This book covers everything you need to know for the CEH exam, making it easy to study without needing to hunt for multiple resources. Dale Meredith's experience and knowledge ensure you are learning from the best. Moreover, the book is updated with the latest exam standards, so you are learning and keeping up with the emerging information. Even practical exercises and real-world examples help you understand the material. So, this book is your ticket to advancing your ethical hacking career. CEHv12- Certified Ethical Hacker This beginner-level book covers all the topics needed to become a certified ethical hacker, making it a one-stop resource. It is the official study material for the CEH certification, so you can trust that it's reliable and aligned with the exam, including practical exercises and labs, solidifying your understanding. You get detailed explanations, examples, and practice questions. This is a straightforward investment if you are interested! CEHv12 – Certified Ethical Hacker: Exam Cram Notes Certified Ethical Hacker: Exam Cram Notes is for beginners. It cuts out the unnecessary stuff and gives you just what you need to know for the exam. Topics are explained in easy language, so you will only waste time studying relevant material. So, if you aim to become a Certified Ethical Hacker, this book is a wise investment to help you ace the exam. Also, this exam cram note is a concise collection of streamlined notes covering the whole exam syllabus. CEH v12 Study Guide with 750 Practice Test Questions This book for advanced learners covers everything you need for the latest CEH exam, with 750 practice questions. It helps you learn practical skills so you are ready even to handle cybersecurity challenges in the real world. Moreover, it is a straightforward way to prepare for the CEH exam and build your skills for a successful cybersecurity career. CEH Certified Ethical Hacker Practice Exams CEH Certified Ethical Hacker Practice Exams is a book for intermediate learners designed to help prepare for the CEH certification exam. It covers all topics for the CEH exam with practice questions to test your knowledge and get comfortable with the exam format. Moreover, questions have explanations, so you understand why specific answers are correct, helping you learn better. This book is a smart buy if you aim for the CEH certification or want to improve your hacking skills. CEH Certified Ethical Hacker Bundle This bundle is vital to becoming proficient in ethical hacking and obtaining CEH certification. It is for intermediate learners, covers essential topics in cybersecurity, is aligned with industry standards, and takes a practical approach to teaching ethical hacking techniques. So, from network security principles to penetration testing methodologies, this book provides a comprehensive overview of key concepts. The Simple CEH Book: Aligned with CEH V12 courseware Aligned with CEH courseware, this book is for mastering ethical hacking. This beginner-level book gives you exactly what you need to ace the CEH certification exam—no extra fluff. With review questions, practice tests, and exam tips, you will be fully prepared for the certification exam. So buy this book for quality content at a fraction of the cost. Selecting the best CEH v12 - Certified Ethical Hacking Course books is paramount for success in the certification exam and beyond. Whether you're a beginner or a seasoned professional, the right study materials can make a significant difference in your understanding of ethical hacking concepts and techniques. By investing in top-rated CEH v12 - Certified Ethical Hacking Course books that offer comprehensive coverage, practical examples, and valuable insights, you can enhance your knowledge, boost your confidence, and ultimately achieve your goal of becoming a Certified Ethical Hacker. With dedication, perseverance, and the right resources at your disposal, you'll be well-equipped to navigate the challenges of the CEH exam and thrive in the dynamic field of cybersecurity. Yes, CEH is still worth it for those pursuing a career in cybersecurity, as it provides foundational knowledge and recognition. However, its value depends on individual career goals, industry demand, and the relevance of other certifications. Consider your specific career path and industry trends before making a decision. 2. Is CEH easier than OSCP? Comparing CEH and OSCP is subjective; CEH is generally considered easier due to its multiple-choice format and broader coverage of topics. OSCP, with its hands-on approach and emphasis on practical skills, is more challenging but offers deeper technical proficiency. 3. Is CEH good for beginners? CEH can be suitable for beginners as it provides foundational knowledge in ethical hacking and cybersecurity concepts. However, beginners should consider hands-on training and practical experience to complement theoretical learning for a well-rounded skill set. 4. Is CEH a hard exam? The difficulty of the CEH exam varies depending on individual preparation, experience, and familiarity with the material. With adequate study and practice, many find the CEH exam manageable, but it can be challenging for those with a limited cybersecurity background. The Motorsport Images Collections captures events from 1895 to today’s most recent coverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors’ Picks.Browse Editors' FavoritesExperience AI-Powered CreativityThe Motorsport Images Collections captures events from 1895 to today’s most recent coverage.Discover The CollectionCurated, compelling, and worth your time. Explore our latest gallery of Editors’ Picks.Browse Editors' FavoritesExperience AI-Powered CreativityDisclosure: Hackr.io is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Explore the platform Having everything in one place is essential. In the past, I’ve worked with MSPs that required different logins for every piece of software – they didn’t offer the visibility and control that we have with Electric. The Electric IT Hub brings together everything we need in one location. From MDM to malware prevention, it’s all integrated and easily managed. B. E.Chief Technology Officer | Fama Technologies Protect your business from cyber attacks Automatic remediation of common security issues Unified visibility of security posture Personalized security plan Access to best-in-class security solutions such as mobile device management, email security, data protection, password management, and more. Start now Gain visibility and control over your IT environment Automated application management Centralized device management Streamlined device procurement Learn more Integrate your IT with the rest of your organization Integration with your HR system Smooth employee on and offboarding Increased team productivity See how Affordable IT and security built for SMBs budget Pay per user and adjust as your business evolves Customized solution based on your business need Explore more Not sure how Electric compares to traditional MSPs? IT solutions matched to your evolving needs Electric partners with industry-leading technology providers to help you manage and secure your business. Mobile device management Anti virus Password management Multi-factor authentication Email security Network security Data backup and recovery Security education HR systems Learn more Ethical hacking is the art of performing hacking in a professional manner as directed by the client. Once completed, the ethical hacker presents a maturity scorecard highlighting your system’s overall risks and vulnerabilities and suggestions to improve. With the steady rise of cybercrime and ransomware attacks such as the recent Kaseya example, companies must upgrade their hack-preventing tactics by adopting innovative technologies to protect their systems instead of falling victim to hackers. What Is Ethical Hacking? Ethical hacking is an authorized attempt to gain unsolicited access to a computer system, data, or application in order to identify security vulnerabilities before malicious attackers can exploit them. Ethical hackers, also known as “white hats,” are security experts who perform these assessments to help improve a company’s security posture. They often work with the approval of the organization before accessing and performing any security assessment. Additionally, an ethical hacker defines the scope of the assessment to ensure that work remains legal and within the client’s approved boundaries. Afterward, they notify the organization of any vulnerability discovered during the assessment and provide remediation advice for mitigating these vulnerabilities. Depending on the data sensitivity, an ethical hacker may have to sign a non-disclosure agreement and any other terms and conditions set by the assessed organization. How to Perform Ethical Hacking Ethical hacking is performed in six basic steps. They include: 1. Reconnaissance Reconnaissance is the principal step where the hacker gathers data about the objective. It involves identifying the target, figuring out the objective’s IP address range, network, DNS records, and other relevant information. 2. Scanning The scanning stage is where the ethical hacker begins to effectively test the objective machine or organization for vulnerabilities that can be exploited. Scanning incorporates the utilization of tools such as network mappers, dialers, port scanners, sweepers, and weakness scanners to gather information. 3. Gaining Access At this stage, the ethical hacker utilizes the information gathered from the checking and scanning stages to outline the organization’s security structure. It’s where the hacker concludes that there are alternatives to accessing the organization’s system. 4. Maintaining Access This is the stage where the ethical hacker has gained access to your framework and now introduces other secondary passages to gain access to the framework in the future. Most ethical hackers use Metasploit in this cycle. 5. Clearing Tracks Clearing tracks is basically an unethical activity that involves erasing logs of the multitude of exercises that happened during the hacking interaction. 6. Reporting The final step of concluding the ethical hacking process is aggregating a report with discoveries made during the hacking interaction. It includes details about the instruments utilized, weaknesses uncovered, the achievement rate, and the mitigation measures. Benefits of Ethical Hacking Cybercrime is skyrocketing amid rising international conflicts. Multiple terrorist organizations fund black hat hackers to promote their illicit grudges with financial motivations or with the aim to compromise national security. The need for ethical hacking has therefore become a necessity. It’s a great way to equip your organization with foolproof defense against evolving threat actors. Primarily, ethical hacking enables you to identify potential cyber attack surfaces before your adversaries do, protecting sensitive data from being misused or stolen. Benefits of ethical hacking include: 1. Identifying Vulnerabilities Ethical hackers perform vulnerability scanning to pinpoint security gaps in an IT infrastructure that malicious hackers could exploit in the real world. They may also use fuzzing to intentionally interfere with your program and its input to crash it, which ultimately reveals any security issues. 2. Preventing Unauthorized Data Access Data security threats and vulnerabilities might extend beyond the firewall guarding your IT infrastructure. To establish an effective data security regime, you may need to challenge your own security construct through critical assessment and testing. Ethical hacking can imitate a criminal hacker’s techniques to help identify and fix the issue. 3. Implementing a Secure Network Through ethical hacking, you can improve your network infrastructure by analyzing and prodding the right architecture to detect vulnerabilities. It helps your organization to build a stronger technical infrastructure by configuring firewalls, protecting network ports, and identifying and implementing the latest network security policies. 4. Preventing a Cyber Attack A successful cyber attack can make your business lose colossal amounts of money, not to mention dented reputation. You may also incur hefty fines due to failure to adhere to safety compliance standards such as GDPR, HIPAA, PCI – DSS, etc. Ethical hacking prevents cyber attacks by informing you about evolving threat vectors and techniques and enabling security professionals to safeguard your IT infrastructure better. What Are the Types of Hackers? Ethical hacking isn’t the only kind of hacking, of course, there are other types of hackers with different intentions. Depending on the intent of hacking a computer system, hackers can be classified into different categories, including white hat, black hat, and grey hat. Here are the most common types of hackers: White Hat Hackers Also referred to as Ethical Hackers, white hat hackers never intend to harm a system but instead try to find weaknesses in a computing system or a network infrastructure. White hat hackers typically perform penetration testing and vulnerability analysis. Black Hat Hackers Black Hat hackers (or crackers) usually hack in order to gain unauthorized access to a computer system and sabotage its operations or steal critical information. Black Hat hacking typically has a bad intent, such as stealing corporate data, damaging the system, violating privacy, blocking network communication, and more. Grey Hat Hackers This type of hacking is a blend of both white hat and black hat hacking techniques. They act for fun and without malicious intent to exploit a security weakness in a system or network without the client’s permission or knowledge. The intent of a grey hat hacker is to bring the weakness to the business owner’s attention and get appreciation or a bounty from the owner. Now that we’ve answered “what is ethical hacking?” you’ve probably realized the importance of cybersecurity, something Electric takes seriously. As the world continues to navigate the complexities of the hybrid workforce, Electric is here to support your organization. While we’re not ethical hackers, Electric can work closely to help you push security policies and configurations that adhere to industry best practices across your entire company. In 2019, Facebook went through the biggest crisis when its user data was breached. Data stemming from the Cultura Colectiva breach was 145GB. It consisted of more than 540 million records including 22,000 unencrypted passwords. Yes, your data might have been breached as well. But how did it happen? The due credit goes to black hat hackers or in simple words, ethical hackers who infiltrated websites and gain unauthorized access into a network to compromise security systems, shut down systems, and alter website functions. What is Ethical Hacking?Ethical hacking is a kind of authorized or legal hacking practice where professionals (ethical hackers) are given special permission in order to gain authorized access for hacking a computer, file, system, application, or data. It is usually done to detect vulnerabilities in software, network system, infrastructure, etc., and to subsequently identify potential data breaches & cyber attacks.With the digital world changing at such a quick pace, there is a growing concern about data breaches at every level. Because everything - personal information, financial information, friends, family, and so on - is shared online, data must be protected at all times. Many hackers are seeking ways to steal personal data for a variety of reasons, such as conflict of interest, national security breaches, terrorist operations, etc. According to a study done by IBM, data breaches cost Indian businesses an average of Rs 17.6 crore in 2022—the highest amount ever recorded. The cost increased 6.6 percent from last year when the average cost of a breach was Rs 16.5 crore. It is up 25 percent from Rs 14 crore in 2020. The same report covered that the global average cost of a data breach reached an all-time high of $4.35 million for surveyed organizations.So, to curb cybercriminal activities, you also need to be thorough with the subject and be an expert white hat hacker in this field. There are primarily 5 types of ethical hacking that you need to be familiar with:Web application hackingWeb server hackingSystem hackingWireless network hackingSocial engineeringTypes of Hackers:White Hat Hackers - The good hackers who exploit security systems to find weaknesses so that the 'bad guys' don't. They are authorized to do so by their respective firms for the express purpose of spotting potential security concerns. Companies that keep sensitive data, such as Google, Facebook, and Microsoft, recruit white-hat hackers.Grey Hat Hackers - Grey-hat hackers are one game ahead of white-hat hackers. They breach networks left and right in order to uncover and rectify flaws in order to steal money from the company. They have no hostile intent and warn authorities and intelligence agencies about security flaws that might be hazardous.Black Hat Hackers - A black hat hacker attempts to obtain illegal access to a network in order to breach security systems, shut down systems, or change website operations. These hackers attempt to get access to personal information, financial information, and passwords.Each type of hacking necessitates certain talents, tools, and procedures, and ethical hackers must think like vicious hackers to tackle problems at full throttle. They must find flaws, understand penetration testing, employ proper tools to carry out the hack, and be prepared. Even if an attack occurs, the damage is relatively low.Best Ethical Hacking Books for Beginner to Advanced Hackers:So, if you want to be an ethical hacker, these 10 ethical hacking books will introduce you to the world of ethical hacking and will help you solve your questions on cybersecurity.1. Hacking: A Beginners’ Guide to Computer Hacking, Basic Security, And Penetration Testing by John SlavioHacking: A Beginners’ Guide to Computer Hacking, Basic Security, And Penetration Testing will teach you all you need to know about hacking, including the history of hacking, the many forms of ethical hacking, and the security precautions you should take. It can also help you get started on your path to becoming an ethical hacker, which is a rapidly developing and in-demand area.The author John Slavio guides you on who and what to watch for in order to prevent hackers from gaining access to your most sensitive information. He discusses the many forms of viruses that may be sent to your computers by crooks breaking into your systems and also informs you about the most prevalent malware, computer viruses, and trojans that can crash your computer or infect it with a virus that can spread to other computers.The author discusses why it is critical to have security software installed on your computer and other systems. This is "the book" for you if you're a newbie in ethical hacking. 2. Hands-on Ethical Hacking and Network Defense by James Corley, Kent Backman, and Michael Simpson Hands-on Ethical Hacking and Network Defense is a strong foundational book for beginners and the best book to learn hacking, including freshers with no knowledge of networking, security, or hacking. The author employs straightforward language and provides extensive explanations of the main ideas. It is mostly a theory book with little application or technical explanation. It is a useful book for a high-level review of hacking ideas such as security testing, various tools, penetration testing approaches, mobile security, and network protection.3. CEH v11 Certified Ethical Hacker Study Guide by Ric MessierThe CEH v11 Certified Ethical Hacker Study Guide provides a thorough understanding of the CEH certification criteria through brief and simple instructions. The chapters are divided by exam objectives, and there is a helpful section that connects each objective to its related chapter. The book covers all themes thoroughly, including difficult chapter review problems and Exam Essentials, a significant feature that indicates essential study areas. Common attack techniques such as reconnaissance and scanning are covered. Intrusion detection, DoS attacks, buffer overflows, wireless assaults, mobile attacks, the Internet of Things (IoT), and other issues are also discussed.4. The Basics of Hacking and Penetration Testing by Patrick EngebretsonIf you want to be a penetration tester (pen-tester), here is a fantastic place to start. Backtrack and Kall Linux, Nmap, Social-Engineer Toolkit, Netcat, and many more technologies are covered in the book. The book is well-organized and covers each topic in detail for a full grasp. The author's tone is lighthearted and engaging. It is a comprehensive ethical hacking training course for novices.5. Hacking: The Art of Exploitation by Jon EricksonThis intermediate hacking book takes a distinct approach to hacking. Apart from knowing networking and security, the author urges you to have a good technological basis and explains how obscure hacking tactics function. This is a hands-on and practical book that explores numerous hacking topics through examples. The author highlights the need of thinking like a hacker, be innovative, and investigate areas that have never been explored before.6. Advanced Penetration Testing: Hacking the world’s most Secure NetworksThe book discusses several challenging problems as well as ways for dealing with them. This course is designed for people who wish to think like professional hackers and do pen-testing on highly protected networks. Many examples in the book make use of C, Java, JavaScript, VBA, Windows Scripting Host, Flash, and other programming languages. In these languages, the author exposes you to a variety of scanning tools and common library programs.7. Exploiting Software: How to Break Code by Greg Hoglund and Gary R. McGrawThe book is very technical and is written in a knowledgeable and informative manner. It is intended for people who have a basic understanding of reverse engineering and exploitation but wish to go deeper into black hat techniques for exploiting software vulnerabilities. The book stresses assault patterns in great depth, something we have not seen in any other literature. The author provides several examples and case studies that are current in nature.8. Penetration Testing – A Hands-On Introduction to HackingThe book begins by outlining the core skills and procedures that every pentester should be familiar with. The book includes many examples, practical teaching using tools, and a machine-based lab, as the title indicates. You'll be able to grasp how a hacker obtains access to security systems, cracks network keys and passwords, and create your own exploits for all of the above and more. Despite the fact that the lab setup is quite outdated in the 1st edition, all of the important material can still be obtained on the web (for example, exploit-DB)- the book is still worthwhile!9. The Web Application Hacker’s Handbook: Finding and Exploiting Security FlawsOne of the commercially successful and popular books for hacking the Web Application Hacker’s Handbook is an efficient approach for people who want to learn about ethical hacking. Here the author has given numerous facts to support his explanations and does not spoon-feed anything. You will learn things by trying several examples and numerous practices and scenarios. The book has many well-organized chapters that provide deep knowledge regarding every topic. Here you will also learn various techniques mentioned for attacking and protecting web applications. The book is good for both beginners and intermediate-level learners. 10. Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition 5th EditionThe book gives the basic knowledge and moves forward towards intermediate level so if you are a fresher or not you will gain benefit from this book. Gray Hat Hacking is an interesting book with crisp and neat examples with all the concepts covered properly which are important for you to start networking, cybersecurity, and ethical hacking. The book has been divided into 5 parts, the first part talks about preparatory work, the second part about core concepts of hacking and penetration testing, the third is about exploiting the system left and right, the fourth covers the advanced analysis of malware and the fifth part is all about IoT which can be hacked. Conclusion:Without a doubt, ethical hacking is a difficult and responsible task. It entails keeping hostile hackers from circumventing security measures and anti-virus software technology. Large corporations spend large sums of money on security specialists and ethical hackers to simulate the exploitation of security system weaknesses. So, have fun learning ethical hacking from these 10 books and start your journey as an ethical hacker in the near future if you haven't yet.