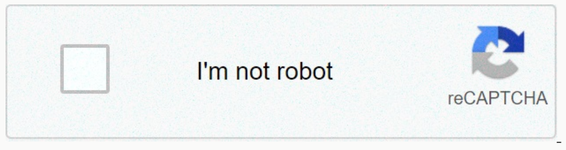


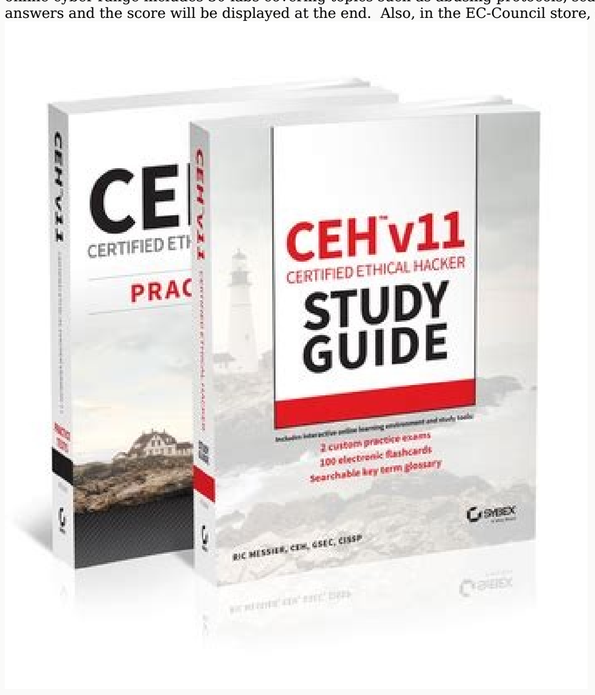
Continue

Ceh v11 book pdf

You're Reading a Free Preview Pages 81 to 90 are not shown in this preview. You're Reading a Free Preview Pages 107 to 172 are not shown in this preview. You're Reading a Free Preview Pages 189 to 230 are not shown in this preview. You're Reading a Free Preview Pages 247 to 283 are not shown in this preview. You're Reading a Free Preview Pages 376 to 425 are not shown in this preview. You're Reading a Free Preview Pages 438 to 479 are not shown in this preview. You're Reading a Free Preview Pages 494 to 508 are not shown in this preview. You're Reading a Free Preview Pages 521 to 542 are not shown in this preview. You're Reading a Free Preview Pages 613 to 632 are not shown in this preview. You're Reading a Free Preview Pages 639 to 652 are not shown in this preview. You're Reading a Free Preview Pages 659 to 676 are not shown in this preview. You're Reading a Free Preview Pages 686 to 695 are not shown in this preview. You're Reading a Free Preview Pages 849 to 1004 are not shown in this preview. You're Reading a Free Preview Pages 1094 to 1491 are not shown in this preview. You're Reading a Free Preview Pages 1657 to 2034 are not shown in this preview. You're Reading a Free Preview Pages 2161 to 2395 are not shown in this preview. You're Reading a Free Preview Pages 2458 to 2638 are not shown in this preview. You're Reading a Free Preview Pages 2701 to 2791 are not shown in this preview. You're Reading a Free Preview Pages 2854 to 3106 are not shown in this preview. As protecting information continues to be a growing concern for today’s businesses, certifications in IT security have become highly desirable, even as the number of certifications has grown. download game mini militia mod apkpure Now you can set yourself apart with the Certified Ethical Hacker (CEH v11) certification. The CEH v11 Certified Ethical Hacker Study Guide offers a comprehensive overview of the CEH certification requirements using concise and easy-to-follow instructions. Chapters are organized by exam objective, with a handy section that maps each objective to its corresponding chapter, so you can keep track of your progress.

The text provides thorough coverage of all topics, along with challenging chapter review questions and Exam Essentials, a key feature that identifies critical study areas. Subjects include common attack practices like reconnaissance and scanning. Also covered are topics like intrusion detection, DoS attacks, buffer overflows, wireless attacks, mobile attacks, Internet of Things (IoT) and more. This study guide goes beyond test prep, providing practical hands-on exercises to reinforce vital skills and real-world scenarios that put what you’ve learned into the context of actual job roles. Gain a unique certification that allows you to function like an attacker, allowing you to identify vulnerabilities so they can be remediated Expand your career opportunities with an IT certificate that satisfies the Department of Defense's 8570 Directive for Information Assurance positions Fully updated for the 2020 CEH v11 exam, including the latest developments in IT security Access the Sybex online learning center, with chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms Thanks to its clear organization, all-inclusive coverage, and practical instruction, the CEH v11 Certified Ethical Hacker Study Guide is an excellent resource for anyone who needs to understand the hacking process or anyone who wants to demonstrate their skills as a Certified Ethical Hacker. Introduction xix Assessment Test xxvi Chapter 1 Ethical Hacking 1 Overview of Ethics 2 Overview of Ethical Hacking 5 Methodologies 6 Cyber Kill Chain 6 Attack Lifecycle 8 Methodology of Ethical Hacking 10 Reconnaissance and Footprinting 10 Scanning and Enumeration 11 Gaining Access 11 Maintaining Access 12 Covering Tracks 12 Summary 13 Chapter 2 Networking Foundations 15 Communications Models 17 Open Systems Interconnection 18 TCP/IP Architecture 21 Topologies 22 Bus Network 22 Star Network 23 Ring Network 24 Mesh Network 25 Hybrid 26 Physical Networking 27 Addressing 27 Switching 28 IP 29 Headers 29 Addressing 31 Subnets 33 TCP 34 UDP 38 Internet Control Message Protocol 39 Network Architectures 40 Network Types 40 Isolation 41 Remote Access 43 Cloud Computing 44 Storage as a Service 45 Infrastructure as a Service 46 Platform as a Service 48 Software as a Service 49 Internet of Things 51 Summary 52 Review Questions 54 Chapter 3 Security Foundations 57 The Triad 59 Confidentiality 59 Integrity 61 Availability 62 Parkerian Hexad 63 Risk 64 Policies, Standards, and Procedures 66 Security Policies 66 Security Standards 67 Procedures 68 Guidelines 68 Organizing Your Protections 69 Security Technology 72 Firewalls 72 Intrusion Detection Systems 77 Intrusion Prevention Systems 80 Endpoint Detection and Response 81 Security Information and Event Management 83 Being Prepared 84 Defense in Depth 84 Defense in Breadth 86 Defensible Network Architecture 87 Logging 88 Auditing 90 Summary 92 Review Questions 93 Chapter 4 Footprinting and Reconnaissance 97 Open Source Intelligence 99 Companies 99 People 108 Social Networking 111 Domain Name System 124 Name Lookups 125 Zone Transfers 130 Passive DNS 133 Passive Reconnaissance 136 Website Intelligence 139 Technology Intelligence 144 Google Hacking 144 Internet of Things (IoT) 146 Summary 148 Review Questions 150 Chapter 5 Scanning Networks 155 Ping Sweeps 157 Using fping 157 Using MegaPing 159 Port Scanning 161 Nmap 162 masscan 176 MegaPing 178 Metasploit 180 Vulnerability Scanning 183 OpenVAS 184 Nessus 196 Looking for Vulnerabilities with Metasploit 202 Packet Crafting and Manipulation 203 hping 204 packETH 207 fragroute 209 Evasion Techniques 211 Protecting and Detecting 214 Summary 215 Review Questions 217 Chapter 6 Enumeration 221 Service Enumeration 223 Remote Procedure Calls 226 SunRPC 226 Remote Method Invocation 228 Server Message Block 232 Built-in Utilities 233 nmap Scripts 237 NetBIOS Enumerator 239 Metasploit 240 Other Utilities 242 Simple Network Management Protocol 245 Simple Mail Transfer Protocol 247 Web-Based Enumeration 250 Summary 257 Review Questions 259 Chapter 7 System Hacking 263 Searching for Exploits 265 System Compromise 269 Metasploit Modules 270 Exploit-DB 274 Gathering Passwords 276 Password Cracking 279 John the Ripper 280 Rainbow Tables 282 Kerberoasting 284 Client-Side Vulnerabilities 289 Living Off the Land 291 Fuzzing 292 Post Exploitation 295 Evasion 295 Privilege Escalation 296 Pivoting 301 Persistence 304 Covering Tracks 307 Summary 313 Review Questions 315 Chapter 8 Malware 319 Malware Types 321 Virus 321 Worm 323 Trojan 324 Botnet 324 Ransomware 326 Dropper 328 Malware Analysis 328 Static Analysis 329 Dynamic Analysis 340 Creating Malware 349 Writing Your Own 350 Using Metasploit 353 Obfuscating 356 Malware Infrastructure 357 Antivirus Solutions 359 Persistence 360 Summary 361 Review Questions 363 Chapter 9 Sniffing 367 Packet Capture 368 tcpdump 369 tshark 376 Wireshark 378 Berkeley Packet Filter 382 Port Mirroring/Spanning 384 Packet Analysis 385 Spoofing Attacks 390 ARP Spoofing 390 DNS Spoofing 394 sslstrip 397 Spoofing Detection 398 Summary 399 Review Questions 402 Chapter 10 Social Engineering 407 Social Engineering 408 Pretexting 410 Social Engineering Vectors 412 Physical Social Engineering 413 Badge Access 413 Man Traps 415 Biometrics 416 Phone Calls 417 Baiting 418 Phishing Attacks 418 Website Attacks 422 Cloning 423 Rogue Attacks 426 Wireless Social Engineering 427 Automating Social Engineering 430 Summary 433 Review Questions 435 Chapter 11 Wireless Security 439 Wi-Fi 440 Wi-Fi Network Types 442 Wi-Fi Authentication 445 Wi-Fi Encryption 446 Bring Your Own Device 450 Wi-Fi Attacks 451 Bluetooth 462 Scanning 463 Bluejacking 465 Bluesnarfing 466 Bluebugging 466 Mobile Devices 466 Mobile Device Attacks 467 Summary 472 Review Questions 474 Chapter 12 Attack and Defense 479 Web Application Attacks 480 XML External Entity Processing 482 Cross-Site Scripting 483 SQL Injection 485 Command Injection 487 File Traversal 489 Web Application Protections 490 Denial-of-Service Attacks 492 Bandwidth Attacks 492 Slow Attacks 495 Legacy 497 Application Exploitation 497 Buffer Overflow 498 Heap Spraying 500 Application Protections and Evasions 501 Lateral Movement 502 Defense in Depth/Defense in Breadth 504 Defensible Network Architecture 506 Summary 508 Review Questions 510 Chapter 13 Cryptography 515 Basic Encryption 517 Substitution Ciphers 517 Diffie-Hellman 520 Symmetric Key Cryptography 521 Data Encryption Standard 522 Advanced Encryption Standard 523 Asymmetric Key Cryptography 524 Hybrid Cryptosystem 525 Nonrepudiation 525 Elliptic Curve Cryptography 526 Certificate Authorities and Key Management 528 Certificate Authority 528 Trusted Third Party 531 Self-Signed Certificates 532 Cryptographic Hashing 534 PGP and S/MIME 536 Disk and File Encryption 538 Summary 541 Review Questions 543 Chapter 14 Security Architecture and Design 547 Data Classification 548 Security Models 550 State Machine 550 Biba 551 Bell-LaPadula 552 Clark-Wilson Integrity Model 552 Application Architecture 553 n-tier Application Design 554 Service-Oriented Architecture 557 Cloud-Based Applications 559 Database Considerations 561 Security Architecture 563 Summary 567 Review Questions 569 Chapter 15 Cloud Computing and the Internet of Things 573 Cloud Computing Overview 574 Cloud Services 578 Shared Responsibility Model 583 Public vs. Private Cloud 585 Cloud Architectures and Deployment 586 Responsive Design 588 Cloud-Native Design 589 Deployment 590 Dealing with REST 593 Common Cloud Threats 598 Access Management 598 Data Breach 600 Web Application Compromise 600 Credential Compromise 602 Insider Threat 604 Internet of Things 604 Operational Technology 610 Summary 612 Review Questions 614 Appendix Answers to Review Questions 617 Chapter 2: Networking Foundations 618 Chapter 3: Security Foundations 619 Chapter 4: Footprinting and Reconnaissance 622 Chapter 5: Scanning Networks 624 Chapter 6: Enumeration 627 Chapter 7: System Hacking 629 Chapter 8: Malware 632 Chapter 9: Sniffing 635 Chapter 10: Social Engineering 636 Chapter 11: Wireless Security 638 Chapter 12: Attack and Defense 641 Chapter 13: Cryptography 643 Chapter 14: Security Architecture and Design 645 Chapter 15: Cloud Computing and the Internet of Things 646 Index 649 The Certified Ethical Hacker (C|EH) certification created by the International Council of E-Commerce Consultants (EC-Council) in 2003 is one of the most popular credentials used to show a person’s competence and know-how in highlighting IT infrastructure weaknesses and vulnerabilities in a legal way and taking action to protect an organization from attacks. A CEH professional working in the information technology or security field plays a key role in protecting a business from cybercrime by using the tools, techniques, and methodologies normally used by hackers to combat active threats that could lead to a network takeover. renault scenic 1999 manual

EC-Council’s CEH certification has helped many expand their professional profiles (see the video testimonials of those who got certified) and take the next step forward in their careers toward becoming ethical hackers. The primary target audience for this type of cert includes security officers, IT auditors and network administrators who have direct oversight of a network structure. The most lucrative job titles for a CEH currently seem to be “information security manager” and “cybersecurity engineer.” To become CEH-certified, professionals must pass a four-hour exam containing 125 multiple-choice questions based on the nine CEH v11 objectives. Cut scores can range from 60% to 85%. Note: EC-Council members holding CEH certifications with at least a 90% score can apply for the CEH Hall of Fame for 2022; a selection committee will carefully review applications based on accomplishments and contributions to society. Successful applicants have a great career transformation story and role in the organization where they are employed. If you’re ready to transition into this role through EC-Council’s Certified Ethical Hacker Certification, you may be wondering what resources are available to help prepare you for the CEH exam. Two of the best books are listed below. CEH Certified Ethical Hacker All-in-One Exam Guide, Fifth Edition, by Matt Walker This book provides up-to-date coverage of every topic on the CEH v11 exam. In this new edition, IT security expert Matt Walker provides in-depth explanations of relevant topics, exam tips, and 300 practice exam questions. Once you’re done with the exam, you will find this guide useful as an on-the-job reference. CEH v11 Certified Ethical Hacker Study Guide, 1st Edition This text offers a comprehensive overview of the CEH certification requirements and thoroughly covers all exam objectives. It also helps identify gaps in knowledge and critical study areas through chapter review questions and “Exam Essentials.” There are practical hands-on exercises, and the book includes access to the Sybex online learning center. What are the best online resources and labs to prepare for the CEH? iLabs CEH This cloud-based subscription service (six months of access to the EC-Council virtual lab environment for CEH) is designed to deliver effective hands-on practice for all the concepts and methodologies covered by the certification in a secure platform. Professionals can safely practice hacking, penetration testing, computer forensics, and secure coding through over 400 complete exercises. Penetration Testing Cyber Range in Infosec Skills The Infosec Skills platform offers a full CEH learning path as well as a Penetration Testing Cyber Range where you can practice your ethical hacking and penetration testing skills. The online cyber range includes 30 labs covering topics such as abusing protocols, scanning for vulnerabilities, identifying exploits and delivering payloads, as well as 4 capture-the-flag (CTF) exercises. What are the best practice exams for the CEH? CEH Exam Prep Start with this practice test by EC-Council. There are 50 questions in this test; the answers and the score will be displayed at the end. Also, in the EC-Council store, you can purchase access to a full year of simulated and progressive assessments to help you experience real exam scenarios.



Measuring your proficiency in each objective as you progress allows you to identify gaps in knowledge easily so that you can focus your studies. Infosec Skills CEH practice exam The Infosec Skills CEH learning path includes a 226-question CEH practice exam. You can also create a customizable CEH practice exam from a pool of more than 1,000 questions. You can adjust the number of questions and the domains of the practice exam to target certain areas of your exam prep. CEH v11: Certified Ethical Hacker Version 11 Practice Tests, 2nd Edition This preparation tool is aligned to the topics covered by the CEH v11 exam; it comes with five complete practice tests that can help professionals steer their study to where it is needed and work with a realistic version of the test. IT security expert Ric Messier provides coverage of all sections of the exam blueprint, thus, giving you the confidence—and skills—needed to pass the CEH test. What are the best online ethical hacking forums?
Although these forums are not related directly to the CEH cert exam, they offer a lot of material for candidates who want to further practice their ethical hacking skills: TechExams Reddit Hackaday HackThisSite Training for the CEH certification exam CEHv11 e-Courseware (digital format and digital lab manual) You can purchase this option with two-year validity and have access to digital material and downloadable tools. Note that an exam voucher is not included. EC-Council’s iClass and iLearn iClass is a training platform that offers a number of solutions catering to any learning style and schedule. It includes live video training courses and tools such as the EC-Council’s Mobile SecurityTool Kit (aka STORM), a pentest platform that comes equipped with STORM Linux on a portable touchscreen device. The iLearn (Self-Study) option, by comparison, is an online, self-paced package of recorded live courses. It offers one-year access to training modules and e-courseware, a virtual lab platform (six months of access), an exam voucher and an attendance certificate.

This asynchronous, self-study environment is available via EC-Council’s ASPEN portal at aspen.eccouncil.org and delivers EC-Council’s sought-after IT security hacking training courses. Accredited Partner training EC-Council has a number of training partners, including Infosec. Infosec offers both a self-paced CEH training option as well as a live online CEH boot camp. Both offerings include access to the CEH practice exams, hands-on labs and other training resources mentioned above. EC-Council IT Security Conference Hacker Halted 2022 is part of the annual series of computer and information security conferences presented by EC-Council. In addition to over 50 presentations from guest speakers, it builds on the educational foundation of EC-Council’s courses in all topics covered by the CEH exam: ethical hacking, computer forensics, pentesting and more. This article has examined some of the best resources available when preparing for the CEH certification, including books, online study resources, practice exams, forums and conferences. Many more resources are available online to meet the different needs of professionals in the field, ranging from webinars to YouTube channels to a number of different types of training courses designed to build your skills and prepare you to pass the CEH exam. Sources: