Click to verify

دليل دراسة comptia security (اختبار الرسمي sy0-501)2

Learn, prepare, and practice for CompTIA Security+ SY0-501 exam success with this full-color CompTIA Authorized Cert Guide, Academic Edition from Pearson IT Certification, a leader in IT Certification learning. This book includes access to four complete practice tests, chapter summaries, and case studies including simulations and hands-on video exercises to reinforce the learning.Master CompTIA's Security+ SY0-501 exam topicsAssess your knowledge with chapter-ending quizzesReinforce your knowledge of key concepts with chapter review activitiesPractice with realistic exam questionsIncludes complete video solutions to hands-on labsPlus interactive simulations on key exam topicsWork through Flash Cards in Q&A and glossary term formatIncludes free access to the Premium Edition eBook You can't perform that action at this time. دورة [illegible] 8 سيوسيلة تمثال إذا كنت تبحث عن دورة متخصصة في مجال الأمن السيبراني، فإن دورة "CompTIA Security+ (SY0-501)" هذه الدورة عبر الإنترنت تستند إلى امتحان [illegible] وإجراء [illegible] وإدارة الهوية والوصول والتشفير والشبكات والأجهزة والبرمجيات، بالإضافة إلى إدارة الهوية والوصول [illegible] هذه الدورة تغطي جميع المجالات السبعة لامتحان CompTIA Security+ SY0-501 وتوفر [illegible] الأساسية لكل مجال. [illegible] تقدم دورة (PKI) معها. تحديد التهديدات الأمنية الأساسية وكيفية الاستجابة لها. إجراء التقييمات الأمنية لتحديد نقاط الضعف. تنفيذ الأمان الخاص بالأجهزة والبرمجيات. إدارة الهوية والوصول. بما في ذلك تكوين الخدمات الدليلية. تحسين تصميم الشبكات لتكون آمنة وتطبيق تقنيات تأمين الشبكة. تعلم أساسيات التشفير وفهم مفاهيم التشفير المتقدمة. تطبيق البنية التحتية للمفتاح العام [illegible] الخدمة التي يعطيها احتمال. SY0-601 بكفاءة [illegible] الأساسية والتشفير [illegible] Security + Exam SY0-601 تعرف على الأهداف الرئيسية والمعايير الأكثر أهمية التي يعطيها integration into your current courses easy and convenientThe uCertify Courses are a foundational learning tool and come with the complete Pearson interactive e-text, pre- and post- assessments, quizzes, exercises, tests, instructional videos, and more. The uCertify Labs and Simulators provide hands-on skills and bridge the gap between conceptual knowledge and real-world application يتميز دليل الدراسة أيضًا إلى أرفف الكتب لكل من تساءل عما إذا كان مجال أمن تكنولوجيا المعلومات مناسب لهم. إنه مرجع لا بد منه - CASP + أو CISSP وكذلك أولئك الذين يأملون في الحصول على شهادة عالية المستوى مثل - SY0-601 تدريب! يتضمن اختبارًا للتقييم المسبق ، وميئات من أسئلة المراجعة ، وامتحانات الممارسة ، والبطاقات التعليمية ، ومسردًا للمصطلحات الأساسية. تمت كتابة الكتاب بطريقة عملية ومباشرة ، مما يضمن لك سهولة تعلم المواد والاحتفاظ بها. مثالي لكل من يخطط لإجراء اختبار Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical study guide! fundamentals of crucial security topics, including the five domains covered by the SY0-601 Exam: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance The study guide comes with the Sybex online, interactive learning environment offering 650 practice questions! Includes a pre-assessment test, hundreds of review questions, practice exams, flashcards, and a glossary of key terms. The book is written in a practical and straightforward manner, ensuring you can easily learn and retain the material, Perfect for everyone planning to take the SY0-601 Exam—as well as those who hope to secure a high-level certification like the CASP+, CISSP, or CISA—the study guide also belongs on the bookshelves of everyone who has ever wondered if the field of IT security is right for them. It's a must-have reference! Interactive learning environment Take your exam prep to the next level with Sybex's superior interactive online study tools. To access our learning environment, simply visit www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and instantly gain one year of FREE access after activation to: Interactive test bank with 2 practice exams to help you identify areas where further review is needed. Get more than 90% of the answers correct, and you're ready to take the certification exam. 100 electronic flashcards to reinforce learning and last-minute prep before the exam Comprehensive glossary in PDF format gives you instant access to the key terms so you are fully prepared اذا اجمل الكتاب فعلاً احفظ على اخيي Nauka o danych425 courses Book ISBN-10: 978-0-7897-5912-2 Learn, prepare, and practice for CompTIA Security+ SY0-501 exam success with this CompTIA Security+ SY0-501 Cert Guide, Academic Edition from Pearson IT Certification, a leader in IT Certification learning. The companion website features three complete practice exams, complete video solutions to hands-on labs, plus interactive flash-based simulations that include drag-and-drop and matching to reinforce the learning.· Master the CompTIA Security+ SY0-501 exam topics· Assess your knowledge with chapter-ending quizzes· Reinforce your knowledge of key concepts with chapter review activities· Practice with realistic exam questions online· Includes complete video solutions to hands-on labs, plus interactive simulations on key exam topics· Work through Flash Cards in Q&A and glossary term format· Includes free access to the Premium Edition eBookCompTIA Security+ SY0-501 Cert Guide, Academic Edition includes video solutions to the hands-on labs, practice tests, and interactive simulations that let the reader learn by doing. Best-selling author and expert instructor David L. Prowse shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics.The book presents you with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter review activities help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your approach to passing the exam.The companion Academic Edition website contains the powerful Pearson Test Prep practice test engine, with three complete practice exams and hundreds of exam-realistic questions and free access to the Premium Edition eBook. The assessment engine offers you a wealth of customization options and reporting features, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. Work through Flash Cards in Q&A and glossary term format to help reinforce your knowledge of key concepts and facts. The Academic Edition companion site also includes complete video solutions to hands-on labs in the book and interactive simulations on key exam topics to reinforce the learning by doing. Learn activities such as testing password strength, matching the type of malware with its definition, finding security issues in the network map, and disallowing a user to access the network on Saturday and Sunday.Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time.The CompTIA study guide helps you master all the topics on the Security+ exam, including· Core computer system security· OS hardening and virtualization· Application security· Network design elements and threats· Perimeter security· Network media and devices security· Physical security and authentication models· Access control· Vulnerability and risk assessment· Monitoring and auditing· Cryptography, including PKI· Redundancy and disaster recovery· Policies and procedures Network Perimeter Security Table of Contents Introduction xxiiChapter 1 Introduction to Security 2Foundation Topics 3Security 101 3 The CIA of Computer Security 3 The Basics of Information Security 4Think Like a Hacker 6Threat Actor Types and Attributes 7Chapter Review Activities 9Chapter 2 Computer Systems Security Part I 12Foundation Topics 13Malicious Software Types 13 Viruses 13 Worms 14 Trojan Horses 14 Ransomware 15 Spyware 15 Rootkits 16 Spam 16 Summary of Malware Threats 17Delivery of Malware 17 Via Software, Messaging, and Media 18 Botnets and Zombies 19 Active Interception 19 Privilege Escalation 19 Backdoors 19 Logic Bombs 20Preventing and Troubleshooting Malware 20 Preventing and Troubleshooting Viruses 20 Preventing and Troubleshooting Worms and Trojans 23 Preventing and Troubleshooting Spyware 24 Preventing and Troubleshooting Rootkits 25 Preventing and Troubleshooting Spam 26 You Can't Save Every Computer from Malware! 27 Summary of Malware Prevention Techniques 27Chapter Review Activities 29Chapter 3 Computer Systems Security Part II 34Foundation Topics 35Implementing Security Applications 35 Personal Software Firewalls 35 Host-Based Intrusion Detection Systems 36 Pop-Up Blockers 38 Data Loss Prevention Systems 38Securing Computer Hardware and Peripherals 39 Securing the BIOS 39 Securing Storage Devices 41 Removable Storage 41 Network Attached Storage 41 Whole Disk Encryption 42 Hardware Security Modules 43 Securing Wireless Peripherals 43Securing Mobile Devices 44 Malware 44 Botnet Activity 45 SIM Cloning and Carrier Unlocking 45 Wireless Attacks 46 Theft 46 Application Security 47 BYOD Concerns 49Chapter Review Activities 53Chapter 4 OS Hardening and Virtualization 58Foundation Topics 59Hardening Operating Systems 59 Removing Unnecessary Applications and Services 59 Windows Update, Patches, and Hotfixes 65 Patches and Hotfixes 66 Patch Management 68 Group Policies, Security Templates, and Configuration Baselines 69 Hardening File Systems and Hard Drives 71Virtualization Technology 74 Types of Virtualization and Their Purposes 74 Hypervisor 75 Securing Virtual Machines 76Chapter Review Activities 79Chapter 5 Application Security 86Foundation Topics 87Securing the Browser 87 General Browser Security Procedures 88 Implement Policies 88 Train Your Users 90 Use a Proxy and Content Filter 91 Secure Against Malicious Code 92 Web Browser Concerns and Security Methods 92 Basic Browser Security 92 Cookies 92 LSOs 93 Add-ons 94 Advanced Browser Security 94Securing Other Applications 95Secure Programming 99 Software Development Life Cycle 99 Core SDLC and DevOps Principles 100 Programming Testing Methods 102 White-box and Black-box Testing 102 Compile-Time Errors Versus Runtime Errors 102 Input Validation 103 Static and Dynamic Code Analysis 104 Fuzz Testing 104 Programming Vulnerabilities and Attacks 104 Backdoors 105 Memory/Buffer Vulnerabilities 105 Arbitrary Code Execution/Remote Code Execution 106 XSS and XSRF 107 More Code Injection Examples 107 Directory Traversal 109 Zero Day Attack 109Chapter Review Activities 111Chapter 6 Network Design Elements 118Foundation Topics 119Network Design 119 The OSI Model 119 Network Devices 120 Switch 120 Bridge 122 Router 122 Network Address Translation, and Private Versus Public IP 123 Network Zones and Interconnections 125 LAN Versus WAN 125 Internet 126 Demilitarized Zone (DMZ) 126 Intranets and Extranets 127 Network Access Control (NAC) 128 Subnetting 128 Virtual Local Area Network (VLAN) 130 Telephony 131 Modems 131 PBX Equipment 132 VoIP 132Cloud Security and Server Defense 133 Cloud Computing 133 Cloud Security 135 Server Defense 137 File Servers 137 Network Controllers 137 E-mail Servers 138 Web Servers 139 FTP Server 140Chapter Review Activities 142Chapter 7 Networking Protocols and Threats 148Foundation Topics 149Ports and Protocols 149 Port Ranges, Inbound Versus Outbound, and Common Ports 149 Protocols That Can Cause Anxiety on the Exam 155Malicious Attacks 155 DoS 155 DDoS 158 Sinkholes and Blackholes 158 Spoofing 159 Session Hijacking 159 Replay 161 Null Sessions 161 Transitive Access and Client-Side Attacks 162 DNS Poisoning and Other DNS Attacks 162 ARP Poisoning 164 Summary of Network Attacks 164Chapter Review Activities 167Chapter 8 Network Perimeter Security 174Foundation Topics 175Firewalls and Network Security 175 Firewalls 175 Proxy Servers 179 Honeypots and Honeynets 181 Data Loss Prevention (DLP) 182NIDS Versus NIPS 183 NIDS 183 NIPS 184 Summary of NIDS Versus NIPS 185 The Protocol Analyzer's Role in NIDS and NIPS 185 Unified Threat Management 186Chapter Review Activities 187Chapter 9 Securing Network Media and Devices 194Foundation Topics 195Securing Wired Networks and Devices 195 Network Device Vulnerabilities 195 Default Accounts 195 Weak Passwords 195 Privilege Escalation 196 Back Doors 197 Network Attacks 197 Other Network Device Considerations 197 Cable Media Vulnerabilities 198 Interference 198 Crosstalk 199 Data Emanation 199 Tapping into Data and Conversations 200Securing Wireless Networks 201 Wireless Access Point Vulnerabilities 202 The Administration Interface 202 SSID Broadcast 202 Rogue Access Points 202 Evil Twin 203 Weak Encryption 203 Wi-Fi Protected Setup 205 Ad Hoc Networks 205 VPN over Open Wireless 205 Wireless Access Point Security Strategies 205 Wireless Transmission Vulnerabilities 208 Bluetooth and Other Wireless Technology Vulnerabilities 209 Bluejacking 209 Bluesnarfing 210 RFID and NFC 210 More Wireless Technologies 210Chapter Review Activities 212Chapter 10 Physical Security and Authentication Models 218Foundation Topics 219Physical Security 219 General Building and Server Room Security 219 Door Access 220 Biometric Readers 221Authentication Models and Components 222 Authentication Models 222 Localized Authentication Technologies 224 802.1X and EAP 224 LDAP 226 Kerberos and Mutual Authentication 227 Remote Desktop Services 229 Remote Authentication Technologies 230 Remote Access Service 230 Virtual Private Networks 231 RADIUS Versus TACACS 234Chapter Review Activities 236Chapter 11 Access Control Methods and Models 244Foundation Topics 245Access Control Models Defined 245 Discretionary Access Control 245 Mandatory Access Control 246 Role-Based Access Control (RBAC) 247 Attribute-based Access Control (ABAC) 248 Access Control Wise Practices 249Rights, Permissions, and Policies 250 Users, Groups, and Permissions 251 Permission Inheritance and Propagation 255 Moving and Copying Folders and Files 256 Usernames and Passwords 256 Policies 258 User Account Control (UAC) 261Chapter Review Activities 262Chapter 12 Vulnerability and Risk Assessment 270Foundation Topics 271Conducting Risk Assessments 271 Qualitative Risk Assessment 272 Quantitative Risk Assessment 273 Security Analysis Methodologies 274 Security Controls 275 Vulnerability Management 276 Penetration Testing 277 OVAL 279 Additional Vulnerabilities 279Assessing Vulnerability with Security Tools 280 Network Mapping 280 Vulnerability Scanning 282 Network Sniffing 283 Password Analysis 284Chapter Review Activities 287Chapter 13 Monitoring and Auditing 294Foundation Topics 295Monitoring Methodologies 295 Signature-Based Monitoring 295 Anomaly-Based Monitoring 295 Behavior-Based Monitoring 296Using Tools to Monitor Systems and Networks 296 Performance Baselining 297 Protocol Analyzers 299 Wireshark 299 SNMP 301 Analytical Tools 302 Use Static and Dynamic Tools 304Conducting Audits 304 Auditing Files 305 Logging 306 Log File Maintenance and Security 310 Auditing System Security Settings 311 SIEM 314Chapter Review Activities 315Chapter 14 Encryption and Hashing Concepts 322Foundation Topics 323Cryptography Concepts 323 Symmetric Versus Asymmetric Key Algorithms 326 Symmetric Key Algorithms 326 Asymmetric Key Algorithms 327 Public Key Cryptography 327 Key Management 328 Steganography 328Encryption Algorithms 329 DES and 3DES 329 AES 329 RC 330 Blowfish and Twofish 331 Summary of Symmetric Algorithms 331 RSA 331 Diffie-Hellman 333 Elliptic Curve 333 More Encryption Types 334 One-Time Pad 334 PGP 335 Pseudorandom Number Generators 336Hashing Basics 336 Cryptographic Hash Functions 337 MD5 338 SHA 338 RIPEMD and HMAC 338 LANMAN, NTLM, and NTLMv2 339 LANMAN 339 NTLM and NTLMv2 340 Hashing Attacks 341 Pass the Hash 341 Happy Birthday! 341 Additional Password Hashing Concepts 342Chapter Review Activities 343Chapter 15 PKI and Encryption Protocols 350Foundation Topics 351Public Key Infrastructure 351 Certificates 351 SSL Certificate Types 352 Single-Sided and Dual-Sided Certificates 352 Certificate Chain of Trust 352 Certificate Formats 352 Certificate Authorities 353 Web of Trust 356Security Protocols 356 S/MIME 357 SSL/TLS 357 SSH 359 PPTP, L2TP, and IPsec 359 PPTP 359 L2TP 359 IPsec 360Chapter Review Activities 361Chapter 16 Redundancy and Disaster Recovery 368Foundation Topics 369Redundancy Planning 369 Redundant Power 370 Redundant Power Supplies 371 Uninterruptible Power Supplies 371 Backup Generators 372 Redundant Data 374 Redundant Networking 376 Redundant Servers 377 Redundant Sites 378 Redundant People 379Disaster Recovery Planning and Procedures 379 Data Backup 379 DR Planning 382Chapter Review Activities 385Chapter 17 Social Engineering, User Education, and Facilities Security 390Foundation Topics 391Social Engineering 391 Pretexting 391 Malicious Insider 391 Diversion Theft 392 Phishing 392 Hoaxes 393 Shoulder Surfing 394 Eavesdropping 394 Dumpster Diving 394 Baiting 394 Piggybacking/Tailgating 394 Watering Hole Attack 395 Summary of Social Engineering Types 395User Education 396 Facilities Security 398 Fire Suppression 398 Fire Extinguishers 398 Sprinkler Systems 399 Special Hazard Protection Systems 399 HVAC 400 Shielding 401 Vehicles 402Chapter Review Activities 404Chapter 18 Policies and Procedures 410Foundation Topics 411Legislative and Organizational Policies 411 Data Sensitivity and Classification of Information 411 Personnel Security Policies 413 Privacy Policies 414 Acceptable Use 414 Change Management 414 Separation of Duties/Job Rotation 415 Mandatory Vacations 415 Onboarding and Offboarding 415 Due Diligence 416 Due Care 416 Due Process 416 User Education and Awareness Training 416 Summary of Personnel Security Policies 417 How to Deal with Vendors 417 How to Dispose of Computers and Other IT Equipment Securely 419Incident Response Procedures 420IT Security Frameworks 424Chapter Review Activities 426Chapter 19 Taking the Real Exam 432 Getting Ready and the Exam Preparation Checklist 432 Tips for Taking the Real Exam 435 Beyond the CompTIA Security+ Certification 438Practice Exam 1: SY0-501 440Glossary 458Elements Available OnlineAppendix A: Answers to the Review QuestionsAnswers to Practice Exam 1View Recommended ResourcesReal-World ScenariosFlash Cards9780789759122 TOC 10/31/2017 0 ratings0% found this document useful (0 votes)873 viewsThis document provides a study guide for the CompTIA Security+ SY0-501 certification exam. It outlines the six domains covered on the exam: 1) Threats, Attacks and Vulnerabilities, 2) Techno...SaveSave Security SY0 501 Study Guide For Later0%0% found this document useful, undefined