Cyberark User Guide Pdf

Insider Threat
HP NonStop Server Security
OCP Oracle Certified Professional Java SE 11 Developer Practice Tests
LATEST CYBERARK DEFENDER + SENTRY (CyberArk CAU302) Exam Practice Questions & Dumps
Whistleblowing for Change
Mastering Linux Security and Hardening
Managing Information Risks
Visual Basic 6.0 Programming By Examples
The IT Leader's Guide to SaaSOps (Volume 1)
Information Systems Security and Privacy
Anbieter von Cloud Speicherdiensten im Überblick
Ransomware
Traction
Mind Tools for Managers
Broken Trust
Privileged Attack Vectors
The Robotic Process Automation Handbook
ServiceNow IT Operations Management
Access Control and Identity Management
What Every Engineer Should Know About Cyber Security and Digital Forensics
Cloud Computing and Services Science
Container Security

Tribe of Hackers
Learning Malware Analysis
Hands-On Red Team Tactics
Hacking Kubernetes
Microsoft Azure Security Center
Computer Safety, Reliability, and Security.
SAFECOMP 2020 Workshops
Kubernetes Security and Observability
Security, Audit and Control Features
SAS For Dummies
Rational Cybersecurity for Business
Computer Security Handbook
Ansible: Up and Running
Learn Helm
How Cybersecurity Really Works
ICCWS 2020 15th International Conference on Cyber Warfare and Security
Learn Kubernetes Security
CISSP: Certified Information Systems Security Professional Study Guide

AVERY CAMERON

Insider Threat Springer Nature
CyberArk Defender + Sentry CAU302 Exam is related to CyberArk Defender + Sentry Certification. This exam validates and measures the Candidates knowledge and deploy, install and configure a basic setup of the CyberArk PAS Solution. It also validates in deploying the CyberArk privileged account security, basic

least privilege access principles & security solution architecture, requirements and workflow. Vault Administrators, IT Personnel, CyberArk PAS Consultants usually hold or pursue this certification and you can expect the same job role after completion of this certification. Preparing for the CyberArk Defender + Sentry certified strength and conditioning specialist exam to become a Certified CyberArk Defender + Sentry CAU302? Here we have brought Best Exam Questions for you so that you can prepare well CyberArk CAU302 exam. Unlike other online simulation practice tests, you get an eBook version that is easy to read & remember these questions. You can simply rely on these questions for successfully certifying this exam.

HP NonStop Server Security "O'Reilly Media, Inc." Turbocharge your marketing plans by making the leap from simple descriptive statistics in Excel to sophisticated predictive analytics with the Python programming language Key FeaturesUse data analytics and machine learning in a sales and marketing contextGain insights from data to make better business decisionsBuild your experience and confidence with realistic hands-on practiceBook Description Unleash the power of data to reach your marketing goals with this practical

guide to data science for business. This book will help you get started on your journey to becoming a master of marketing analytics with Python. You'll work with relevant datasets and build your practical skills by tackling engaging exercises and activities that simulate real-world market analysis projects. You'll learn to think like a data scientist, build your problem-solving skills, and discover how to look at data in new ways to deliver business insights and make intelligent data-driven decisions. As well as learning how to clean, explore, and visualize data, you'll implement machine learning algorithms and build models to make predictions. As you work through the book, you'll use Python tools to analyze sales, visualize advertising data, predict revenue, address customer churn, and implement customer segmentation to understand behavior. By the end of this book, you'll have the knowledge, skills, and confidence to implement data science and machine learning techniques to better understand your marketing data and improve your decision-making. What you will learnLoad, clean, and explore sales and marketing data using pandasForm and test hypotheses using real data sets and analytics toolsVisualize patterns in customer behavior using MatplotlibUse advanced machine learning models like random forest and

SVMUse various unsupervised learning algorithms for customer segmentationUse supervised learning techniques for sales predictionEvaluate and compare different models to get the best outcomesOptimize models with hyperparameter tuning and SMOTEWho this book is for This marketing book is for anyone who wants to learn how to use Python for cutting-edge marketing analytics. Whether you're a developer who wants to move into marketing, or a marketing analyst who wants to learn more sophisticated tools and techniques, this book will get you on the right path. Basic prior knowledge of Python and experience working with data will help you access this book more easily.

OCP Oracle Certified Professional Java SE 11 Developer Practice Tests John Wiley & Sons

Align your business requirements with IT by implementing ServiceNow IT Operations with ease. About This Book Written to the latest specification, it will cover basic to advanced concepts and architecture. Take a service-centric approach to operations management and consolidate all your resource data into a single system IT record. Beat the key challenge of managing multiple business operations (even running globally) over a complex IT infrastructure and see

immediate results. Who This Book Is For The book is aimed at System administrators, IT operations and IT managers who plan to implement ServiceNow IT Operations Management for their organization. They have no knowledge of ServiceNow ITOM. What You Will Learn Step by step guide in setting up each features with in ServiceNow ITOM Install and configure the required application or plugin Integrate with other provider services as deemed appropriate Explore Orchestration capabilities and how to analyze the data Learn about the ServiceNow graphical interface Integrate with other applications within ServiceNow Aims to cover the fundamentals concepts to advanced concepts Best practices and advanced features In Detail ServiceNow ITOM enables infrastructure and processes to be managed in a highly automated manner. It contains various segments that ensure its applications and enterprise infrastructures are optimized for high performance and helps in creating a lean and agile organization through service-level visibility and automation. This book will be a comprehensive guide that will be based on Geneva release and will help you discover how IT activities can be connected to your business needs, rather than just focusing on internal IT process. It

will take a service-centric approach to operations management and consolidate all your resource data into a single system IT record. You will learn about discovery, orchestration, MID server and cloud management, helping you take full advantage of ServiceNow IT Operations Management to improve the quality of service & increasing the service availability. By the end of the book, you will be able to achieve improved service availability, immediate visibility of vital business services and much more, all from the convenience of your single screen. Style and approach This will be a step by step learning guide helping readers to implement ServiceNow IT Operations Management for their organization.

LATEST CYBERARK DEFENDER + SENTRY (CyberArk CAU302) Exam Practice Questions & Dumps Apress

Your one-stop guide to learning and implementing Red Team tactics effectively Key FeaturesTarget a complex enterprise environment in a Red Team activityDetect threats and respond to them with a real-world cyber-attack simulationExplore advanced penetration testing tools and techniquesBook Description Red Teaming is used to enhance security by performing simulated attacks on an organization in order to

detect network and system vulnerabilities. Hands-On Red Team Tactics starts with an overview of pentesting and Red Teaming, before giving you an introduction to few of the latest pentesting tools. We will then move on to exploring Metasploit and getting to grips with Armitage. Once you have studied the fundamentals, you will learn how to use Cobalt Strike and how to set up its team server. The book introduces some common lesser known techniques for pivoting and how to pivot over SSH, before using Cobalt Strike to pivot. This comprehensive guide demonstrates advanced methods of post-exploitation using Cobalt Strike and introduces you to Command and Control (C2) servers and redirectors. All this will help you achieve persistence using beacons and data exfiltration, and will also give you the chance to run through the methodology to use Red Team activity tools such as Empire during a Red Team activity on Active Directory and Domain Controller. In addition to this, you will explore maintaining persistent access, staying untraceable, and getting reverse connections over different C2 covert channels. By the end of this book, you will have learned about advanced penetration testing tools, techniques to get reverse shells over encrypted channels, and processes for post-exploitation. What you

will learnGet started with red team engagements using lesser-known methodsExplore intermediate and advanced levels of post-exploitation techniquesGet acquainted with all the tools and frameworks included in the Metasploit frameworkDiscover the art of getting stealthy access to systems via Red TeamingUnderstand the concept of redirectors to add further anonymity to your C2Get to grips with different uncommon techniques for data exfiltrationWho this book is for Hands-On Red Team Tactics is for you if you are an IT professional, pentester, security consultant, or ethical hacker interested in the IT security domain and wants to go beyond Penetration Testing. Prior knowledge of penetration testing is beneficial.

Whistleblowing for Change John Wiley & Sons

The manager's must-have guide to excelling in all aspects of the job Mind Tools for Managers helps new and experienced leaders develop the skills they need to be more effective in everything they do. It brings together the 100 most important leadership skills—as voted for by 15,000 managers and professionals worldwide—into a single volume, providing an easy-access solutions manual for people wanting to be the best

manager they can be. Each chapter details a related group of skills, providing links to additional resources as needed, plus the tools you need to put ideas into practice. Read beginning-to-end, this guide provides a crash course on the essential skills of any effective manager; used as a reference, its clear organization allows you to find the solution you need quickly and easily. Success in a leadership position comes from results, and results come from the effective coordination of often competing needs: your organization, your client, your team, and your projects. These all demand time, attention, and energy, and keeping everything running smoothly while making the important decisions is a lot to handle. This book shows you how to manage it all, and manage it well, with practical wisdom and expert guidance. Build your ideal team and keep them motivated Make better decisions and boost your strategy game Manage both time and stress to get more done with less Master effective communication, facilitate innovation, and much more Managers wear many hats and often operate under a tremendously diverse set of job duties. Delegation, prioritization, strategy, decision making, communication, problem solving, creativity, time management, project management and stress management are all part of your

domain. Mind Tools for Managers helps you take control and get the best out of your team, your time, and yourself.

Mastering Linux Security and Hardening Microsoft Press

This book constitutes extended, revised and selected papers from the 9th International Conference on Cloud Computing and Services Science, CLOSER 2019, held in Heraklion, Greece, in May 2019.The 11 papers presented in this volume were carefully reviewed and selected from a total of 102 submissions. CLOSER 2019 focuses on the emerging area of Cloud Computing, inspired by some latest advances that concern the infrastructure, operations, and available servicesthrough the global network.

Managing Information Risks Sergey Skudaev

OVER 1 MILLION COPIES SOLD! Do you have a grip on your business, or does your business have a grip on you? All entrepreneurs and business leaders face similar frustrations—personnel conflict, profit woes, and inadequate growth. Decisions never seem to get made, or, once made, fail to be properly implemented. But there is a solution. It's not complicated or theoretical.The Entrepreneurial Operating System® is a practical method for achieving the business success you have always envisioned. More than 80,000 companies have

discovered what EOS can do. In Traction, you'll learn the secrets of strengthening the six key components of your business. You'll discover simple yet powerful ways to run your company that will give you and your leadership team more focus, more growth, and more enjoyment. Successful companies are applying Traction every day to run profitable, frustration-free businesses—and you can too. For an illustrative, real-world lesson on how to apply Traction to your business, check out its companion book, Get A Grip.

Visual Basic 6.0 Programming By Examples Wiley

Want to run your Kubernetes workloads safely and securely? This practical book provides a threat-based guide to Kubernetes security. Each chapter examines a particular component's architecture and potential default settings and then reviews existing high-profile attacks and historical Common Vulnerabilities and Exposures (CVEs). Authors Andrew Martin and Michael Hausenblas share best-practice configuration to help you harden clusters from possible angles of attack. This book begins with a vanilla Kubernetes installation with built-in defaults. You'll examine an abstract threat model of a distributed system running arbitrary workloads, and then progress to a detailed assessment of each

component of a secure Kubernetes system. Understand where your Kubernetes system is vulnerable with threat modelling techniques Focus on pods, from configurations to attacks and defenses Secure your cluster and workload traffic Define and enforce policy with RBAC, OPA, and Kyverno Dive deep into sandboxing and isolation techniques Learn how to detect and mitigate supply chain attacks Explore filesystems, volumes, and sensitive information at rest Discover what can go wrong when running multitenant workloads in a cluster Learn what you can do if someone breaks in despite you having controls in place

The IT Leader's Guide to SaaSOps

(Volume 1) Packt Publishing Ltd Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and

private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common

encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

Information Systems Security and Privacy Universitätsverlag Potsdam

Managing Information Risks: Threats, Vulnerabilities, and Responses identifies and categorizes risks related to creation, collection, storage, retention, retrieval, disclosure and ownership of information in organizations of all types and sizes. It is intended for risk managers, information governance specialists, compliance officers, attorneys, records managers, archivists, and other decision-makers, managers, and analysts who are responsible for risk management initiatives related to their organizations' information assets. An opening chapter

defines and discusses risk terminology and concepts that are essential for understanding, assessing, and controlling information risk. Subsequent chapters provide detailed explanations of specific threats to an organization's information assets, an assessment of vulnerabilities that the threats can exploit, and a review of available options to address the threats and their associated vulnerabilities. Applicable laws, regulations, and standards are cited at appropriate points in the text. Each chapter includes extensive endnotes that support specific points and provide suggestions for further reading. While the book is grounded in scholarship, the treatment is practical rather than theoretical. Each chapter focuses on knowledge and recommendations that readers can use to: heighten risk awareness within their organizations, identify threats and their associated consequences, assess vulnerabilities, evaluate risk mitigation options, define risk-related responsibilities, and align information-related initiatives and activities with their organizations' risk management strategies and policies. Compared to other works, this book deals with a broader range of information risks and draws on ideas from a greater variety of disciplines, including business process management, law,

financial analysis, records management, information science, and archival administration. Most books on this topic associate information risk with digital data, information technology, and cyber security. This book covers risks to information of any type in any format, including paper and photographic records as well as digital content.

Anbieter von Cloud Speicherdiensten im Überblick ISACA

This book constitutes the proceedings of the Workshops held in conjunction with SAFECOMP 2020, 39th International Conference on Computer Safety, Reliability and Security, Lisbon, Portugal, September 2020. The 26 regular papers included in this volume were carefully reviewed and selected from 45 submissions; the book also contains one invited paper. The workshops included in this volume are: DECSoS 2020: 15th Workshop on Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems. DepDevOps 2020: First International Workshop on Dependable Development-Operation Continuum Methods for Dependable Cyber-Physical Systems. USDAI 2020: First International Workshop on Underpinnings for Safe Distributed AI. WAISE 2020: Third International Workshop on Artificial Intelligence Safety Engineering. The workshops were

held virtually due to the COVID-19 pandemic. *Ransomware* Jones & Bartlett Learning Totally updated for 2011, here's the ultimate study guide for the CISSP exam Considered the most desired certification for IT security professionals, the Certified Information Systems Security Professional designation is also a career-booster. This comprehensive study guide covers every aspect of the 2011 exam and the latest revision of the CISSP body of knowledge. It offers advice on how to pass each section of the exam and features expanded coverage of biometrics, auditing and accountability, software security testing, and other key topics. Included is a CD with two full-length, 250-question sample exams to test your progress. CISSP certification identifies the ultimate IT security professional; this complete study guide is fully updated to cover all the objectives of the 2011 CISSP exam Provides in-depth knowledge of access control, application development security, business continuity and disaster recovery planning, cryptography, Information Security governance and risk management, operations security, physical (environmental) security, security architecture and design, and telecommunications and network security Also covers legal and

regulatory investigation and compliance Includes two practice exams and challenging review questions on the CD Professionals seeking the CISSP certification will boost their chances of success with CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition.

Traction Springer Nature

Discover high-value Azure security insights, tips, and operational optimizations This book presents comprehensive Azure Security Center techniques for safeguarding cloud and hybrid environments. Leading Microsoft security and cloud experts Yuri Diogenes and Dr. Thomas Shinder show how to apply Azure Security Center's full spectrum of features and capabilities to address protection, detection, and response in key operational scenarios. You'll learn how to secure any Azure workload, and optimize virtually all facets of modern security, from policies and identity to incident response and risk management. Whatever your role in Azure security, you'll learn how to save hours, days, or even weeks by solving problems in most efficient, reliable ways possible. Two of Microsoft's leading cloud security experts show how to: • Assess the impact of cloud and hybrid environments on security, compliance, operations, data protection, and risk management • Master

a new security paradigm for a world without traditional perimeters • Gain visibility and control to secure compute, network, storage, and application workloads • Incorporate Azure Security Center into your security operations center • Integrate Azure Security Center with Azure AD Identity Protection Center and third-party solutions • Adapt Azure Security Center's built-in policies and definitions for your organization • Perform security assessments and implement Azure Security Center recommendations • Use incident response features to detect, investigate, and address threats • Create high-fidelity fusion alerts to focus attention on your most urgent security issues • Implement application whitelisting and just-in-time VM access • Monitor user behavior and access, and investigate compromised or misused credentials • Customize and perform operating system security baseline assessments • Leverage integrated threat intelligence to identify known bad actors

Mind Tools for Managers Packt Publishing Ltd

To facilitate scalability and resilience, many organizations now run applications in cloud native environments using containers and orchestration. But how do you know if the deployment is secure? This practical book examines key

underlying technologies to help developers, operators, and security professionals assess security risks and determine appropriate solutions. Author Liz Rice, Chief Open Source Officer at Isovalent, looks at how the building blocks commonly used in container-based systems are constructed in Linux. You'll understand what's happening when you deploy containers and learn how to assess potential security risks that could affect your deployments. If you run container applications with kubectl or docker and use Linux command-line tools such as ps and grep, you're ready to get started. Explore attack vectors that affect container deployments Dive into the Linux constructs that underpin containers Examine measures for hardening containers Understand how misconfigurations can compromise container isolation Learn best practices for building container images Identify container images that have known software vulnerabilities Leverage secure connections between containers Use security tooling to prevent attacks on your deployment

Broken Trust Elsevier

While Robotic Process Automation (RPA) has been around for about 20 years, it has hit an inflection point because of the convergence of cloud computing, big data

and AI. This book shows you how to leverage RPA effectively in your company to automate repetitive and rules-based processes, such as scheduling, inputting/transferring data, cut and paste, filling out forms, and search. Using practical aspects of implementing the technology (based on case studies and industry best practices), you'll see how companies have been able to realize substantial ROI (Return On Investment) with their implementations, such as by lessening the need for hiring or outsourcing. By understanding the core concepts of RPA, you'll also see that the technology significantly increases compliance – leading to fewer issues with regulations – and minimizes costly errors. RPA software revenues have recently soared by over 60 percent, which is the fastest ramp in the tech industry, and they are expected to exceed $1 billion by the end of 2019. It is generally seamless with legacy IT environments, making it easier for companies to pursue a strategy of digital transformation and can even be a gateway to AI. The Robotic Process Automation Handbook puts everything you need to know into one place to be a part of this wave. What You'll Learn Develop the right strategy and planDeal with resistance and fears from employeesTake an in-depth look at the leading RPA systems,

including where they are most effective, the risks and the costsEvaluate an RPA system Who This Book Is For IT specialists and managers at mid-to-large companies *Privileged Attack Vectors* Packt Publishing Ltd Insider Threat: Detection, Mitigation, Deterrence and Prevention presents a set of solutions to address the increase in cases of insider threat. This includes espionage, embezzlement, sabotage, fraud, intellectual property theft, and research and development theft from current or former employees. This book outlines a step-by-step path for developing an insider threat program within any organization, focusing on management and employee engagement, as well as ethical, legal, and privacy concerns. In addition, it includes tactics on how to collect, correlate, and visualize potential risk indicators into a seamless system for protecting an organization’s critical assets from malicious, complacent, and ignorant insiders. Insider Threat presents robust mitigation strategies that will interrupt the forward motion of a potential insider who intends to do harm to a company or its employees, as well as an understanding of supply chain risk and cyber security, as they relate to insider threat. Offers an ideal resource for executives and managers who

want the latest information available on protecting their organization’s assets from this growing threat Shows how departments across an entire organization can bring disparate, but related, information together to promote the early identification of insider threats Provides an in-depth explanation of mitigating supply chain risk Outlines progressive approaches to cyber security

The Robotic Process Automation Handbook "O'Reilly Media, Inc."

Durch die immer stärker werdende Flut an digitalen Informationen basieren immer mehr Anwendungen auf der Nutzung von kostengünstigen Cloud Storage Diensten. Die Anzahl der Anbieter, die diese Dienste zur Verfügung stellen, hat sich in den letzten Jahren deutlich erhöht. Um den passenden Anbieter für eine Anwendung zu finden, müssen verschiedene Kriterien individuell berücksichtigt werden. In der vorliegenden Studie wird eine Auswahl an Anbietern etablierter Basic Storage Diensten vorgestellt und miteinander verglichen. Für die Gegenüberstellung werden Kriterien extrahiert, welche bei jedem der untersuchten Anbieter anwendbar sind und somit eine möglichst objektive Beurteilung erlauben. Hierzu gehören unter anderem Kosten, Recht, Sicherheit,

Leistungsfähigkeit sowie bereitgestellte Schnittstellen. Die vorgestellten Kriterien können genutzt werden, um Cloud Storage Anbieter bezüglich eines konkreten Anwendungsfalles zu bewerten. *ServiceNow IT Operations Management* Academic Conferences and publishing limited Securing, observing, and troubleshooting containerized workloads on Kubernetes can be daunting. It requires a range of considerations, from infrastructure choices and cluster configuration to deployment controls and runtime and network security. With this practical book, you'll learn how to adopt a holistic security and observability strategy for building and securing cloud native applications running on Kubernetes. Whether you're already working on cloud native applications or are in the process of migrating to its architecture, this guide introduces key security and observability concepts and best practices to help you unleash the power of cloud native applications. Authors Brendan Creane and Amit Gupta from Tigera take you through the full breadth of new cloud native approaches for establishing security and observability for applications running on Kubernetes. Learn why you need a security and observability

strategy for cloud native applications and determine your scope of coverage Understand key concepts behind the book's security and observability approach Explore the technology choices available to support this strategy Discover how to share security responsibilities across multiple teams or roles Learn how to architect Kubernetes security and observability for multicloud and hybrid environments

Access Control and Identity Management

CRC Press

Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781119643371) was previously published as Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781793464187). While this version features a new cover design and introduction, the remaining content is the same as the prior release and should not be considered a new or updated product. Looking for real-world advice from leading cybersecurity experts? You've found your tribe. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World is your guide to joining the ranks of hundreds of thousands of cybersecurity professionals around the world. Whether you're just joining the industry, climbing the corporate ladder, or considering consulting, Tribe of Hackers offers the practical know-how, industry

perspectives, and technical insight you need to succeed in the rapidly growing information security market. This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world's most noteworthy hackers and influential security specialists.

What Every Engineer Should Know About Cyber Security and Digital Forensics

John Wiley & Sons

Visual Basic is one of the easiest to learn computer programming language. Yes, it is obsolete but all MS Office products include VBA (Visual Basic for Application) and if you

learn VB you will know VBA! In my tutorial, I used VB 6 to explain step by step how to create a simple Visual Basic Application and a relatively complex one (a Patient Management system) that is using a database. A patient Management application source code is explained in details. You will learn how to design and create a database in MS Access and how to create tables and queries. The book includes a sample application that shows how to use Windows API function. You will learn how to convert VB program that can be run only in Visual Basic development environment to a distributable application that can be installed on any client computer. For illustration, I included more than 100 screenshot images and links to a video. You will be able to download from my website complete source code for 7 Visual Basic projects including a Password Keeper, a Patient Management and a Billing Management application. Get Your Copy Today