Dvr Password Reset Service

Learn how to troubleshoot Windows 10 the way the experts do, whatever device or form-factor you're using. Focus on the problems that most commonly plague PC users and fix each one with a step-by-step approach that helps you understand the cause, the solution, and the tools required. Discover the connections between the different hardware and software in your devices, and how their bonds with external hardware, networks, and the Internet are more dependent than you think, and learn how to build resilience into any computer system, network, or device running Windows 10. If you're fed up of those nagging day-to-day issues, want to avoid costly repairs, or just want to learn more about how PCs work, Windows 10 Troubleshooting is your ideal one-stop guide to the Windows 10 operating system. What You Will Learn: Understand your PC's ecosystem and how to connect the dots, so you can successfully track problems to their source Create resilient backups of your operating system, files, and documents, and enable quick and easy restore Learn your way around Windows' built-in administration tools, to quickly fix the typical problems that come up Diagnose and repair a wide range of common problems with printers and other essential peripherals Solve complex startup problems that can prevent a PC form booting Make your PC safe and secure for the whole family, and for everybody in your workplace Understand the threat from malware and viruses and a range of approaches to dealing with them, depending on the situation Bomb-proof your PC with

advanced security, group policy, and firewall policies Learn the top Tips and tricks for researching difficult problems, including third-party tools and useful web resources Work with the registry, file system, and Sysinternals to troubleshooting PCs in the workplace Who This Book Is For: Anyone using Windows 10 on a desktop, laptop, or hybrid device

Step by step guide to connecting all your electronic devices into one network A home network allows you to share Internet connections, photos, video, music, game consoles, printers, and other electronic gadgets. This do-it-yourself guide shows you step by step how to create a wired or wireless network in your home. In the For Dummies tradition of making technology less intimidating, Home Networking Do-It-Yourself For Dummies breaks down the process into easy steps with clear instructions. Increasing broadband speeds, cellular technology, the explosive growth of iPhone sales, and the new Home Group feature in Windows 7 all contribute to a booming interest in home networking This step-by-step guide walks do-it-yourselfers through the process of setting up a wired or wireless network with Windows 7 and Windows Vista Demonstrates how to connect desktops or laptops, printers, a home server, a router, high-speed Internet access, a video game system, a telephone line, and entertainment peripherals Shows how to share files, music, and video, and connect to an iPhone Provides maintenance and troubleshooting tips Home Networking Do-It-Yourself For Dummies enables you to take advantage of everything a home network can offer without hiring a technology wizard.

Presents information on getting the most out of a PC's hardware and software, covering such topics as upgrading the BIOS, configuring the hard drive, installing more RAM, improving CPU performance, and adding COM ports.

Published in February 1917 in a secret edition strictly limited to 700 copies on security grounds, this immensely detailed manual, backed up by scores of photographs, drawings, plans and diagrams, gives the reader a complete run-down on everything that British Intelligence knew about enemy Zeppelins. Based largely on the examination of two sister 'super Zeppelins' - L31 and L33 - shot down over England, the book has chapters on evolving Zeppelin types, training and personnel; the building of Zeppelins; and their machinery and propellors; Fabric and hydrogen gas valves; bomb dropping gear; wireless telegraph apparatus; bombs, flares, guns and ammunition; bomb and machine gun sights; compasses, lifeboats, fire extinguishers and other safety equipment; and weather conditions. Although the loss of life and material damage inflicted by the Zeppelins was quite light, as a psychological weapon their effect was profound and induced near-panic, particularly as Britain had at first no answer to them. Gradually, however, blackouts were introduced, along with searchlights ringing London and squadrons briefed to intercept and shoot down the gigantic airships. The war against the Zeppelin would be won, but before they gave way to bombers the 'Zepp' had left an indelible mark on aviation history.

Professional ASP.NET 3.5 Security, Membership, and

Role Management with C# and VB
Windows XP Annoyances
Design and Implementation
Lucifer Christ Encounters
Electrical Engineering Regulations
Home Networking Do-It-Yourself For Dummies

This is a practical manual on operating systems, which describes a small UNIX-like operating system, demonstrating how it works and illustrating the principles underlying it. The relevant sections of the MINIX source code are described in detail, and the book has been revised to include updates in MINIX, which initially started as a v7 unix clone for a floppy-disk only 8088. It is now aimed at 386, 486 and pentium machines, and is based on the international posix standard instead of on v7. Versions of MINIX are now also available for the Macintosh and SPARC.

Presents fifty hacks to customize performance of a Mac, including automating tasks, increasing security, playing Wii games, and modifying wifi.

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not

usually covered in classical computer forensics. This guide attempts to bridge that gap by providing an in-depth look into mobile phones and explaining the technologies involved and their relationship to forensic procedures. It covers phones with features beyond simple voice communication and text messaging and their technical and operating characteristics. This guide also discusses procedures for the preservation, acquisition, examination, analysis, and reporting of digital information present on cell phones, as well as available forensic software tools that support those activities.

This IBM® Redbooks® publication consolidates, in one document, detailed descriptions of the hardware configurations and options offered as part of the IBM System Storage DS5000 families of products. This edition covers updates and additional functions available with the IBM System Storage DS® Storage Manager Version 10.77 (firmware level 7.77). This book presents the concepts and functions used in planning and managing the storage servers, such as multipathing and path failover. The book offers a step-by-step guide to using the Storage Manager to create arrays, logical drives, and other basic (as well as advanced)

management tasks. This publication also contains practical information about diagnostics and troubleshooting, and includes practical examples of how to use scripts and the command-line interface. This publication is intended for customers, IBM Business Partners, and IBM technical professionals who want to learn more about the capabilities and advanced functions of the DS5000 series of storage servers with Storage Manager Software V10.77. It also targets those who have a DS5000 storage subsystem and need detailed advice about how to configure it. This book is designed specifically to address the hardware features and configuration of the IBM System Storage DS5000 family and can be used in conjunction with the following IBM Redbooks publications: IBM System Storage DS5000 Series Implementation and Best Practices Guide, SG24-8024 IBM System Storage DS Storage Manager Copy Services Guide, SG24-7822

Painless web apps with React, JSX, Redux, and GraphQL

EJ Girl Hero #6

Video Surveillance of Nesting Birds

Privileged Attack Vectors

Practical Mobile Forensics

Click Here to Kill Everybody: Security and

Survival in a Hyper-connected World

This is a biography of the author's encounters with the Super Natural.

NEW YORK TIMES BESTSELLER "A hands-on, real talk guide for navigating the hot-button issues that so many families struggle with" - Reese Witherspoon Do you find yourself taking on the lion's share of all the thankless, invisible but time-consuming work in the home? FAIR PLAY is the first book that shows you that there can be a different way: a way to get more done, with less fuss, in a way that feels more balanced. Eve Rodsky is changing society one relationship at a time, by coming up with a 21st-century solution to an age-old problem: women shouldering the brunt of domestic responsibilities, the mental load, the emotional labour. Everything that is required to keep the fridge full, the children's homework in their bags, and the household running. The unequal division of all this invisible work in relationships is a recipe for disaster, but no one has offered a real solution to this dilemma, until now. Eve Rodsky was tired of always being the one who has to remember to buy loo roll, or to book the family's dentist appointments, or to send the thank you cards - all while working full time. So Eve decided to do what she does every day as an organisational management consultant: Organise. She conducted original research with more than 500 couples to figure out WHAT the invisible work in a family actually is and HOW to get it done effectively and all in a way that makes relationships even stronger. FAIR PLAY identifies the 100 main tasks in any relationship, and then divides those tasks fairly (not

necessarily equally) so that both parties contribute their fair share. If we don't learn to rebalance our home life and reclaim some time to develop the skills and passions that keep us unique, then we risk losing our right to be interesting, not just to our partner, but to ourselves. Getting this right isn't a luxury, it's a necessity for a happy, lasting partnership. Part how-to guide for couples, part modern relationship manifesto, FAIR PLAY offers an innovative system with a completely original lexicon to discuss how relationships actually work ... and how we can make them work better.

Covering up-to-date mobile platforms, this book focuses on teaching you the most recent tools and techniques for investigating mobile devices. Readers will delve into a variety of mobile forensics techniques for iOS 11-13, Android 8-10 devices, and Windows 10.

This IBM Redpaper publication presents and positions the DS8910F Model 993 storage system. This modular system can be integrated into a 16U contiguous space of an IBM z15TM model T02 or IBM z14® Model ZR1 with Feature Code 0937 and IBM LinuxONE III model LT2 or LinuxONE Rockhopper II model LR1 with Feature Code 0938. The DS8910F Model 993 allows you to take advantage of the performance boost of all-flash systems and advanced features while limiting data center footprint and power infrastructure requirements.

Fair Play

React Quickly

On the Ball

Surveillance Camera Code of Practice

Information Security Policies and Actions in Modern

Integrated Systems

IBM DS8870 Architecture and Implementation (Release 7.5)

This IBM® Redbooks® publication describes the concepts, architecture, and implementation of the IBM DS8870. The WhitepaperRedpaperbook provides reference information to assist readers who need to plan for, install, and configure the DS8870. The IBM DS8870 is the most advanced model in the IBM DS8000® series and is equipped with IBM POWER7+TM based controllers. Various configuration options are available that scale from dual 2-core systems up to dual 16-core systems with up to 1 TB of cache. The DS8870 features an integrated High-Performance Flash Enclosure (HPFE) with flash cards that can deliver up to 250,000 IOPS and up to 3.4 GBps bandwidth. A High-Performance All-Flash configuration is also available. The DS8870 now features 16 Gbps host adapters. Connectivity options, with up to 128 Fibre Channel/IBM FICON® ports for host connections, make the DS8870 suitable for multiple server environments in open systems and IBM zTM Systems environments. DS8870 Release 7.5 brings new and enhanced IBM z SystemsTM synergy features. These features are covered in detail in IBM DS8870 and IBM z Systems Synergy,

REDP-5186. The DS8870 supports advanced disaster recovery solutions, business continuity solutions, and thin provisioning. All disk drives in the DS8870 storage system have the Full Disk Encryption (FDE) feature. The DS8870 also can be integrated in a Lightweight Directory Access Protocol (LDAP) infrastructure. The DS8870 can automatically optimize the use of each storage tier, particularly flash drives and flash cards, through the IBM Easy Tier® feature, which is available at no extra charge. This edition applies the IBM DS8870 Release 7.5.

This IBM® RedpaperRedbooks® publication describes the concepts, architecture, and implementation of the IBM DS8900F family. The WhitepaperRedpaperbook provides reference information to assist readers who need to plan for, install, and configure the DS8900F systems. This edition applies to DS8900F systems with IBM DS8000® Licensed Machine Code (LMC) 7.9.20 (bundle version 89.20.xx.x), referred to as Release 9.2. The DS8900F is an all-flash system exclusively, and it offers three classes: DS8980F: Analytic Class: The DS8980F Analytic Class offers best performance for organizations that want to expand their workload

possibilities to artificial intelligence (AI), Business Intelligence (BI), and machine learning (ML). IBM DS8950F: Agility Class all-flash: The Agility Class consolidates all your mission-critical workloads for IBM Z®, IBM LinuxONE, IBM Power Systems, and distributed environments under a single all-flash storage solution.. IBM DS8910F: Flexibility Class all-flash: The Flexibility Class reduces complexity while addressing various workloads at the lowest DS8900F family entry cost. . TThe DS8900F architecture relies on powerful IBM POWER9TM processor-based servers that manage the cache to streamline disk input/output (I/O), which maximizes performance and throughput. These capabilities are further enhanced by High-Performance Flash Enclosures (HPFE) Gen2. Like its predecessors, the DS8900F supports advanced disaster recovery (DR) solutions, business continuity solutions, and thin provisioning. The IBM DS8910F Rack-Mounted model 993 is described in IBM DS8910F Model 993 Rack-Mounted Storage System Release 9.1, REDP-5566.

Summary React Quickly is for anyone who wants to learn React.js fast. This hands-on book teaches you the concepts you need with lots of examples, tutorials, and a

large main project that gets built throughout the book. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Successful user interfaces need to be visually interesting, fast, and flowing. The React.js JavaScript library supercharges view-heavy web applications by improving data flow between UI components. React sites update visual elements efficiently and smoothly, minimizing page reloads. React is developer friendly, with a strong ecosystem to support the dev process along the full application stack. And because it's all JavaScript, React is instantly familiar. About the Book React Quickly is the tutorial for web developers who want to get started fast with React.js. Following carefully chosen and clearly explained examples, you'll learn React development using your existing JavaScript and web dev skills. You'll explore a host of different projects as you learn about web components, forms, and data. What's Inside Master React fundamentals Build full web apps with data and routing Test components Optimize React apps About the Reader This book is for developers comfortable building web applications with

JavaScript. About the Author Azat Mardan is a Tech Fellow at Capital One with extensive experience using and teaching JavaScript and Node, and author of several books on JavaScript, Node, React, and Express. Table of Contens PART 1 - REACT FOUNDATION Meeting React Baby steps with React Introduction to JSX Making React interactive with states React component lifecycle events Handling events in React Working with forms in React Scaling React components Project: Menu component Project: Tooltip component Project: Timer component PART 2 - REACT ARCHITECTURE The Webpack build tool React routing Working with data using Redux Working with data using GraphQL Unit testing React with Jest React on Node and Universal JavaScript Project: Building a bookstore with React Router Project: Checking passwords with Jest Project: Implementing autocomplete with Jest, Express, and MongoDB APPENDIXES Appendix A - Installing applications used in this book Appendix B - React cheatsheet Appendix C - Express.js cheatsheet Appendix D - MongoDB and Mongoose cheatsheet Appendix E - ES6 for success This work has been selected by scholars as being culturally important and is part of the knowledge base of civilization as we know it. This work is in the public domain

in the United States of America, and possibly other nations. Within the United States, you may freely copy and distribute this work, as no entity (individual or corporate) has a copyright on the body of the work. Scholars believe, and we concur, that this work is important enough to be preserved, reproduced, and made generally available to the public. To ensure a quality reading experience, this work has been proofread and republished using a format that seamlessly blends the original graphical elements with text in an easy-to-read typeface. We appreciate your support of the preservation process, and thank you for being an important part of keeping this knowledge alive and relevant.

Sandworm

Knuckleheads in the News

Operating Systems

TiVo Hacks

Driver CPC - the Official DVSA Guide for Professional Goods Vehicle Drivers

Mac Hacks

Explains how to configure Windows XP for maximum control and flexibility, work effectively with the Registry, take advantage of the built-in firewall, and troubleshoot problems.

The book is an easy-to-follow guide with clear instructions on various mobile forensic techniques. The chapters and the topics within are structured for

a smooth learning curve, which will swiftly empower you to master mobile forensics. If you are a budding forensic analyst, consultant, engineer, or a forensic professional wanting to expand your skillset, this is the book for you. The book will also be beneficial to those with an interest in mobile forensics or wanting to find data lost on mobile devices. It will be helpful to be familiar with forensics in general but no prior experience is required to follow this book.

A world of "smart" devices means the Internet can kill people. We need to act. Now. Everything is a computer. Ovens are computers that make things hot; refrigerators are computers that keep things cold. These computers—from home thermostats to chemical plants—are all online. The Internet, once a virtual abstraction, can now sense and touch the physical world. As we open our lives to this future, often called the Internet of Things, we are beginning to see its enormous potential in ideas like driverless cars, smart cities, and personal agents equipped with their own behavioral algorithms. But every knife cuts two ways. All computers can be hacked. And Internet-connected computers are the most vulnerable. Forget data theft: cutting-edge digital attackers can now crash your car, your pacemaker, and the nation's power grid. In Click Here to Kill Everybody, renowned expert and best-selling author Bruce Schneier examines the hidden risks of this new reality. After exploring the full implications of a world populated by hyperconnected devices, Schneier reveals the hidden web of technical,

political, and market forces that underpin the pervasive insecurities of today. He then offers common-sense choices for companies, governments, and individuals that can allow us to enjoy the benefits of this omnipotent age without falling prey to its vulnerabilities. From principles for a more resilient Internet of Things, to a recipe for sane government regulation and oversight, to a better way to understand a truly new environment, Schneier's vision is required reading for anyone invested in human flourishing.

There is a spy at the Shine agency's top-secret training camp... Agent EJ12 needs to find out who the spy is and locate the missing SHINE gadget invention. That's the easy part. As EJ12, Emma Jacks can do anything. So why is she so worried about trying out for the school soccer team? Perhaps she isn't after all...

How to Identify & Resolve Radio-tv Interference Problems

A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

Letters of Brunswick and Hessian Officers During the American Revolution

Share the mental load, rebalance your relationship and transform your life

Guidelines on Cell Phone Forensics

YOU CAN'T MAKE THIS STUFF UP! Here is a hilarious collection that catches real-life knuckleheads in outrageous acts of brazen

*stupidity, giving new meaning to that famous four-letter word: "DUH"! * The Oregon resident who was waxing his 1984 Pontiac--and somehow managed to shove the antenna up his nose . . . GRANDMOTHER OF EIGHT MAKES HOLE IN ONE * The Atlanta Braves pitcher who was treated for five-inch-long welts after he tried to iron his polo shirt while wearing it . . . MINERS REFUSE TO WORK AFTER DEATH * The inmate at a Chesapeake Correctional Facility who filed a five million dollar lawsuit against himself . . . DRUNK GETS NINE MONTHS IN VIOLIN CASE * The woman who couldn't stand the discomfort of having a callus on her right foot, so she blew off her big toe with a shotgun . . . Radio personality John "Kato" Machay's lively compilation of news stories, headlines, and courtroom gaffes proves hands down that truth is dumber than fiction! REMEMBER: To err may be human, but to laugh out loud is divine.*

Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration testers must master Kali's varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You'll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you're new to the

field or an established pentester, you'll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral movement, and privilege escalation Apply practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python

This official book is specifically designed to help prepare goods vehicle drivers for their Driver Certificate of Professional Competence (Driver CPC) test. The book focuses on case studies and vehicle safety demonstrations..

TiVo Hacks helps you get the most out of your TiVo personal video recorder. Armed with just a screwdriver and basic understanding of PC hardware (or willingness to learn), preeminent hackability awaits. This book includes hacks for changing the order of recorded programs, activating the 30-second skip to blaze through commercials, upgrading TiVo's hard drive for more hours of recording, use of TiVo's Home Media Option to remotely schedule a recording via the Web, log in to the serial port for command-line access to programming data, log files, closed-captioning data, display graphics on the TiVo

screen, and even play MP3s.Readers who use advanced hacks to put TiVo on their home network via the serial port, Ethernet, USB, or wireless (with 802.11b WiFi) will watch a whole new world open up. By installing various open source software packages, you can use TiVo for mail, instant messaging, caller-ID, and more. It's also easy to run a web server on TiVo to schedule recordings, access lists of recorded shows, and even display them on a web site. While TiVo gives viewers personalized control of their TVs, TiVo Hacks gives users personalized control of TiVo.Note: Not all TiVos are the same. The original TiVo, the Series 1, is the most hackable TiVo out there; it's a box thrown together with commodity parts and the TiVo code is running on open hardware. The Series 2 TiVo, the most commonly sold TiVo today, is not open. You won't see hacks in this book that involve modifying Series 2 software.

Successful IoT Device/Edge and Platform Security Deployment

Battery Hazards

Demystifying Internet of Things Security

100 Industrial-Strength Tips & Tools

Tips & Tools for Unlocking the Power of OS X Mountain Lion

New Worksight

Professional ASP.NET 3.5 Security, Membership, and Role Management with C# and VBJohn Wiley & SonsHome Networking Do-It-Yourself For DummiesJohn Wiley & Sons

Break down the misconceptions of the Internet of Things by examining the different security building blocks available in Intel

Architecture (IA) based IoT platforms. This open access book reviews the threat pyramid, secure boot, chain of trust, and the SW stack leading up to defense-in-depth. The IoT presents unique challenges in implementing security and Intel has both CPU and Isolated Security Engine capabilities to simplify it. This book explores the challenges to secure these devices to make them immune to different threats originating from within and outside the network. The requirements and robustness rules to protect the assets vary greatly and there is no single blanket solution approach to implement security. Demystifying Internet of Things Security provides clarity to industry professionals and provides and overview of different security solutions What You'll Learn Secure devices, immunizing them against different threats originating from inside and outside the networkGather an overview of the different security building blocks available in Intel Architecture (IA) based IoT platformsUnderstand the threat pyramid, secure boot, chain of trust, and the software stack leading up to defense-in-depth Who This Book Is For Strategists, developers, architects, and managers in the embedded and Internet of Things (IoT) space trying to understand and implement the security in the IoT devices/platforms.

This code of practice provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities in England and Wales who must have regard to the code when exercising any functions to which the code relates. Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the code voluntarily. The purpose of the code will be to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them. Sections cover the background, purpose of the code, scope of the surveillance activity to which this code applies and effect of the code. Chapters include an overview and guiding principles; the development or use of surveillance camera systems; the use or

processing of images or other information obtained by virtue of such systems, and the Surveillance Camera Commissioner.

This work discusses research in theoretical and practical aspects of security in distributed systems, in particular in information systems and related security tools. Topics include XML-based management systems, security of multimedia data, and technology and use of smart cards.

IBM DS8910F Model 993 Rack-Mounted Storage System Release 9.1

IBM System Storage DS5000 Series Hardware Guide

PC Hacks

British Jewry Book of Honour 1914-1918

IBM DS8900F Architecture and Implementation: Updated for Release 9.2

IP Video Surveillance. An Essential Guide.

The true story of the most devastating cyberattack in history and the desperate hunt to identify and track the elite Russian agents behind it, from Wired senior writer Andy Greenberg. "Lays out in chilling detail how future wars will be waged in cyberspace and makes the case that we have done little, as of yet, to prevent it." —Washington Post In 2014, the world witnessed the start of a mysterious series of cyberattacks. Targeting American utility companies, NATO, and electric grids in Eastern Europe, the strikes grew ever more brazen. They culminated in the summer of 2017, when the malware known as NotPetya was unleashed, penetrating, disrupting, and paralyzing some of the world's largest

businesses—from drug manufacturers to software developers to shipping companies. At the attack's epicenter in Ukraine, ATMs froze. The railway and postal systems shut down. Hospitals went dark. NotPetya spread around the world, inflicting an unprecedented ten billion dollars in damage—the largest, most destructive cyberattack the world had ever seen. The hackers behind these attacks are quickly gaining a reputation as the most dangerous team of cyberwarriors in history: a group known as Sandworm. Working in the service of Russia's military intelligence agency, they represent a persistent, highly skilled force, one whose talents are matched by their willingness to launch broad, unrestrained attacks on the most critical infrastructure of their adversaries. They target government and private sector, military and civilians alike. A chilling, globe-spanning detective story, Sandworm considers the danger this force poses to our national security and stability. As the Kremlin's role in foreign government manipulation comes into greater focus, Sandworm exposes the realities not just of Russia's global digital offensive, but of an era where warfare ceases to be waged on the battlefield. It reveals how the lines between digital and physical conflict, between

wartime and peacetime, have begun to blur—with world-shaking implications.
Expertly guides the novice and the more experienced turner step-by-step through 15 graded exercises and projects.
See how privileges, insecure passwords, administrative rights, and remote access can be combined as an attack vector to breach any organization. Cyber attacks continue to increase in volume and sophistication. It is not a matter of if, but when, your organization will be breached. Threat actors target the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today's environmental complexity has seen an explosion of privileged credentials for many different account types such as domain and local administrators, operating systems (Windows, Unix, Linux, macOS, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and so many more. When unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. We are experiencing an expanding universe of privileged accounts almost everywhere. There is no one solution

or strategy to provide the protection you need against all vectors and stages of an attack. And while some new and innovative products will help protect against or detect against a privilege attack, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. Privileged Attack Vectors details the risks associated with poor privilege management, the techniques that threat actors leverage, and the defensive measures that organizations should adopt to protect against an incident, protect against lateral movement, and improve the ability to detect malicious activity due to the inappropriate usage of privileged credentials. This revised and expanded second edition covers new attack vectors, has updated definitions for privileged access management (PAM), new strategies for defense, tested empirical steps for a successful implementation, and includes new disciplines for least privilege endpoint management and privileged remote access. What You Will Learn Know how identities, accounts, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and

monitoring strategies to mitigate privilege threats and risk Understand a 10-step universal privilege management implementation plan to guide you through a successful privilege access management journey Develop a comprehensive model for documenting risk, compliance, and reporting based on privilege session activity Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privilege access management problems

This IBM® Redbooks® publication describes the concepts, architecture, and implementation of the IBM System Storage® DS8700 storage subsystem. This book has reference information that will help you plan for, install, and configure the DS8700 and also discusses the architecture and components. The DS8700 is the most advanced model in the IBM System Storage DS8000® series. It includes IBM POWER6®-based controllers, with a dual 2-way or dual 4-way processor complex implementation. Its extended connectivity, with up to 128 Fibre Channel/FICON® ports for host connections, make it suitable for multiple server environments in both open systems and IBM System z® environments. If desired, the

DS8700 can be integrated in an LDAP infrastructure. The DS8700 supports thin provisioning. Depending on your specific needs, the DS8700 storage subsystem can be equipped with SATA drives, FC drives, and Solid® State Drives (SSDs). The DS8700 can now automatically optimize the use of SSD drives through its no charge Easy Tier feature. The DS8700 also supports Full Disk Encryption (FDE) feature. Its switched Fibre Channel architecture, dual processor complex implementation, high availability design, and the advanced Point-in-Time Copy and Remote Mirror and Copy functions that incorporates make the DS8700 storage subsystem suitable for mission-critical business functions.

Building Effective Cyber-Defense Strategies to Protect Organizations

Kali Linux Penetration Testing Bible

Windows 10 Troubleshooting

IBM System Storage DS8700 Architecture and Implementation

Asian Sources Electronics

Forensically investigate and analyze iOS, Android, and Windows 10 devices, 4th Edition

Declining bird populations, especially those that breed in North American grasslands, have stimulated extensive research on factors that affect nest

failure and reduced reproductive success. Until now, this research has been hampered by the difficulties inherent in observing nest activities. Video Surveillance of Nesting Birds highlights the use of miniature video cameras and recording equipment yielding new important and some unanticipated insights into breeding bird biology, including previously undocumented observations of hatching, incubation, fledging, diurnal and nocturnal activity patterns, predator identification, predator-prey interactions, and cause-specific rates of nest loss. This seminal contribution to bird reproductive biology uses tools capable of generating astonishing results with the potential for fresh insights into bird conservation, management, and theory.

[Commercial Reciprocity Between the United States and the British North American Provinces] [microform]

The Fundamentals of Woodturning

[memorandum of the British Plenipoteniaries: Full Text of the Old Reciprocity Treaty of 1854: Full Text of the Proposed New Treaty]