

# Beginning Linux Antivirus Development The Story A

Right here, we have countless ebook **Beginning Linux Antivirus Development The Story A** and collections to check out. We additionally meet the expense of variant types and with type of the books to browse. The pleasing book, fiction, history, novel, scientific research, as skillfully as various other sorts of books are readily within reach here.

As this Beginning Linux Antivirus Development The Story A, it ends occurring visceral one of the favored books Beginning Linux Antivirus Development The Story A collections that we have. This is why you remain in the best website to look the incredible books to have.

*Wireshark for Security Professionals* - Jessey Bullock 2017-03-20

Master Wireshark to solve real-world security problems If you don't already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. Wireshark for Security Professionals covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with Wireshark. Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wireshark's features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The book's final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark Explore the virtual w4sp-lab environment that mimics a real-world network Gain experience using the Debian-based Kali OS among other systems Understand the technical details behind network attacks Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark Employ Lua to extend Wireshark features and create useful scripts To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark.

Computerworld - 2004-05-10

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

*Open Source Intelligence Methods and Tools* - Nihad A. Hassan 2018-06-30

Apply Open Source Intelligence (OSINT) techniques, methods, and tools to acquire information from publicly available online sources to support your intelligence analysis. Use the harvested data in different scenarios such as financial, crime, and terrorism investigations as well as performing business competition analysis and acquiring intelligence about individuals and other entities. This book will also improve your skills to acquire information

online from both the regular Internet as well as the hidden web through its two sub-layers: the deep web and the dark web. The author includes many OSINT resources that can be used by intelligence agencies as well as by enterprises to monitor trends on a global level, identify risks, and gather competitor intelligence so more effective decisions can be made. You will discover techniques, methods, and tools that are equally used by hackers and penetration testers to gather intelligence about a specific target online. And you will be aware of how OSINT resources can be used in conducting social engineering attacks. Open Source Intelligence Methods and Tools takes a practical approach and lists hundreds of OSINT resources that can be used to gather intelligence from online public sources. The book also covers how to anonymize your digital identity online so you can conduct your searching activities without revealing your identity. What You'll Learn Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making in your organization Use OSINT resources to protect individuals and enterprises by discovering data that is online, exposed, and sensitive and hide the data before it is revealed by outside attackers Gather corporate intelligence about business competitors and predict future market directions Conduct advanced searches to gather intelligence from social media sites such as Facebook and Twitter Understand the different layers that make up the Internet and how to search within the invisible web which contains both the deep and the dark webs Who This Book Is For Penetration testers, digital forensics investigators, intelligence services, military, law enforcement, UN agencies, and for-profit/non-profit enterprises

**Practical Reverse Engineering** - Bruce Dang 2014-02-03

Analyzing how hacks are done, so as to stop them in the future Reverse engineering is the process of analyzing hardware or software and understanding it, without having access to the source code or design documents. Hackers are able to reverse engineer systems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. Practical Reverse Engineering goes under the hood of reverse engineering for security analysts, security engineers, and system programmers, so they can learn how to use these same processes to stop hackers in their tracks. The book covers x86, x64, and ARM (the first book to cover all three); Windows kernel-mode code rootkits and drivers; virtual machine protection techniques; and much more. Best of all, it offers a systematic approach to the material, with plenty of hands-on exercises and real-world examples. Offers a systematic approach to understanding reverse engineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architectures as well as deobfuscation and virtual machine protection techniques Provides special coverage of Windows kernel-mode code (rootkits/drivers), a topic not often covered elsewhere, and explains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, Windows Kernel, and Reversing Tools provides crucial, up-to-date guidance for a broad range of IT professionals.

Computerworld - 2005-02-14

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**CIO** - 2008-02

PC Mag - 2008-03

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

*Learning Linux Binary Analysis* - Ryan "elfmaster" O'Neill 2016-02-29

Uncover the secrets of Linux binary analysis with this handy guide About This Book Grasp the intricacies of the ELF binary format of UNIX and Linux Design tools for reverse engineering and binary forensic analysis Insights into UNIX and Linux memory infections, ELF viruses, and binary protection schemes Who This Book Is For If you are a software engineer or reverse engineer and want to learn more about Linux binary analysis, this book will provide you with all you need to implement solutions for binary analysis in areas of security, forensics, and antivirus. This book is great for both security enthusiasts and system level engineers. Some experience with the C programming language and the Linux command line is assumed. What You Will Learn Explore the internal workings of the ELF binary format Discover techniques for UNIX Virus infection and analysis Work with binary hardening and software anti-tamper methods Patch executables and process memory Bypass anti-debugging measures used in malware Perform advanced forensic analysis of binaries Design ELF-related tools in the C language Learn to operate on memory with ptrace In Detail Learning Linux Binary Analysis is packed with knowledge and code that will teach you the inner workings of the ELF format, and the methods used by hackers and security analysts for virus analysis, binary patching, software protection and more. This book will start by taking you through UNIX/Linux object utilities, and will move on to teaching you all about the ELF specimen. You will learn about process tracing, and will explore the different types of Linux and UNIX viruses, and how you can make use of ELF Virus Technology to deal with them. The latter half of the book discusses the usage of Kprobe instrumentation for kernel hacking, code patching, and debugging. You will discover how to detect and disinfect kernel-mode rootkits, and move on to analyze static code. Finally, you will be walked through complex userspace memory infection analysis. This book will lead you into territory that is uncharted even by some experts; right into the world of the computer hacker. Style and approach The material in this book provides detailed insight into the arcane arts of hacking, coding, reverse engineering Linux executables, and dissecting process memory. In the computer security industry these skills are priceless, and scarce. The tutorials are filled with knowledge gained through first hand experience, and are complemented with frequent examples including source code.

Penetration Testing - Georgia Weidman 2014-06-14

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual

assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

**PC Mag** - 2000-06-27

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

Rootkits and Bootkits - Alex Matrosov 2019-05-07

Rootkits and Bootkits will teach you how to understand and counter sophisticated, advanced threats buried deep in a machine's boot process or UEFI firmware. With the aid of numerous case studies and professional research from three of the world's leading security experts, you'll trace malware development over time from rootkits like TDL3 to present-day UEFI implants and examine how they infect a system, persist through reboot, and evade security software. As you inspect and dissect real malware, you'll learn: • How Windows boots—including 32-bit, 64-bit, and UEFI mode—and where to find vulnerabilities • The details of boot process security mechanisms like Secure Boot, including an overview of Virtual Secure Mode (VSM) and Device Guard • Reverse engineering and forensic techniques for analyzing real malware, including bootkits like Rovnix/Carberp, Gapz, TDL4, and the infamous rootkits TDL3 and Festi • How to perform static and dynamic analysis using emulation and tools like Bochs and IDA Pro • How to better understand the delivery stage of threats against BIOS and UEFI firmware in order to create detection capabilities • How to use virtualization tools like VMware Workstation to reverse engineer bootkits and the Intel Chipsec tool to dig into forensic analysis Cybercrime syndicates and malicious actors will continue to write ever more persistent and covert attacks, but the game is not lost. Explore the cutting edge of malware analysis with Rootkits and Bootkits. Covers boot processes for Windows 32-bit and 64-bit operating systems.

CIO - 2008-02-15

**Beginning Linux Antivirus Development** - Ian Lee 2017-12-14

This is the world's first book that you have never read on how to develop security software. It is said that we are striding into the initial era of the internet of things, but I believe we are in the middle of the IoT now. Smart watches, tablets for note-taking in class, Smart TVs allowing us to see popular soap dramas, game consoles to play games with your friends, e-books you read before you go to bed and smartphones you always look at to name but a few. We are using different types of computer systems which are all connected day and night. But, have you ever wondered how many gadgets among those things are applied to security technologies? In reality, not many devices are introduced to the technologies. Also, many people say that security is important in the era of IoT while they tell us that it is essential that the vulnerability of IoT should be removed. So much so that, they focus on getting rid of vulnerabilities. Of course, the concentration of vulnerability can't be ruled out. But, adding a new feature to software breed another new vulnerability. Even so, security technologies for commercial antivirus programs can't apply to all IoT devices. If that's the case, what if IoT software developers create a security function for their devices on their own and apply it to theirs? This is the first book that navigates you through the detail on

how to develop security software functions. What you can get from this book. While you are reading this book, you will find yourself to implement a simple antivirus software and an antivirus server by yourself. You may be still wondering if that is going to happen to you. You can check out a demo video at the website as below. I am sure that you will be encouraged to do the same after watching it.

<http://www.schoolime.com/securityschool/antivirus/demo/> You might think that this book simply explains code like any other books. The answer is no. This is a story about a student with no experience in security who grows into a security software developer. Starting with a plausible hacking incident, the main character in this book collects requirements, draws a design and writes code. By doing so, he goes through the entire process. You can also get the knowledge as below after you finish this book. - The basics of antivirus structure - Requirement-driven development - Practical software design using UML - How to modify kernels for security Don't worry, any developers can read this book. You can be a security software developer. Do you think those words are tricky for you? No worries. This book walks you through every process so that anyone who has the basic knowledge as below can easily understand the book. You will find yourself to be a security software developer after finishing this book. - C programming - Simple echo socket programming - UML (It's enough to hear of it. No necessary to handle it) - The role of Linux kernels (No necessary to develop it) There is a first for everyone.

**Computer Security Basics** - Rick Lehtinen 2006-06-13

This is the must-have book for a must-know field. Today, general security knowledge is mandatory, and, if you who need to understand the fundamentals, Computer Security Basics 2nd Edition is the book to consult. The new edition builds on the well-established principles developed in the original edition and thoroughly updates that core knowledge. For anyone involved with computer security, including security administrators, system administrators, developers, and IT managers, Computer Security Basics 2nd Edition offers a clear overview of the security concepts you need to know, including access controls, malicious software, security policy, cryptography, biometrics, as well as government regulations and standards. This handbook describes complicated concepts such as trusted systems, encryption, and mandatory access control in simple terms. It tells you what you need to know to understand the basics of computer security, and it will help you persuade your employees to practice safe computing. Topics include: Computer security concepts Security breaches, such as viruses and other malicious programs Access controls Security policy Web attacks Communications and network security Encryption Physical security and biometrics Wireless network security Computer security and requirements of the Orange Book OSI Model and TEMPEST

*Machine Learning for Computer and Cyber Security* - Brij B. Gupta 2019-02-05

While Computer Security is a broader term which incorporates technologies, protocols, standards and policies to ensure the security of the computing systems including the computer hardware, software and the information stored in it, Cyber Security is a specific, growing field to protect computer networks (offline and online) from unauthorized access, botnets, phishing scams, etc. Machine learning is a branch of Computer Science which enables computing machines to adopt new behaviors on the basis of observable and verifiable data and information. It can be applied to ensure the security of the computers and the information by detecting anomalies using data mining and other such techniques. This book will be an invaluable resource to understand the importance of machine learning and data mining in establishing computer and cyber security. It emphasizes important security aspects associated with computer and cyber security along with the analysis of machine learning and data mining based solutions. The book also highlights the future research domains in which these solutions can be applied.

Furthermore, it caters to the needs of IT professionals, researchers, faculty members, scientists, graduate students, research scholars and software developers who seek to carry out research and develop combating solutions in the area of cyber security using machine learning based approaches. It is an extensive source of information for the

readers belonging to the field of Computer Science and Engineering, and Cyber Security professionals. Key Features: This book contains examples and illustrations to demonstrate the principles, algorithms, challenges and applications of machine learning and data mining for computer and cyber security. It showcases important security aspects and current trends in the field. It provides an insight of the future research directions in the field. Contents of this book help to prepare the students for exercising better defense in terms of understanding the motivation of the attackers and how to deal with and mitigate the situation using machine learning based approaches in better manner.

**PC Mag** - 2003-04-22

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

**Network World** - 2001-12-24

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

*Network World* - 2003-03-03

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

**InfoWorld** - 1999-12-27

InfoWorld is targeted to Senior IT professionals. Content is segmented into Channels and Topic Centers. InfoWorld also celebrates people, companies, and projects.

**Computerworld** - 2004-02-02

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**The Security Development Lifecycle** - Michael Howard 2006

Your customers demand and deserve better security and privacy in their software. This book is the first to detail a rigorous, proven methodology that measurably minimizes security bugs--the Security Development Lifecycle (SDL). In this long-awaited book, security experts Michael Howard and Steve Lipner from the Microsoft Security Engineering Team guide you through each stage of the SDL--from education and design to testing and post-release. You get their first-hand insights, best practices, a practical history of the SDL, and lessons to help you implement the SDL in any development organization. Discover how to: Use a streamlined risk-analysis process to find security design issues before code is committed Apply secure-coding best practices and a proven testing process Conduct a final security review before a product ships Arm customers with prescriptive guidance to configure and deploy your product more securely Establish a plan to respond to new security vulnerabilities Integrate security discipline into agile methods and processes, such as Extreme Programming and Scrum Includes a CD featuring: A six-part security class video conducted by the authors and other Microsoft security experts Sample SDL documents and fuzz testing tool PLUS--Get book updates on the Web. For customers who purchase an ebook version of this title, instructions for downloading the CD files can be found in the ebook.

**Computerworld** - 2005-10-10

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**CSO** - 2002-10

The business to business trade publication for information and physical Security professionals.

**PC Mag** - 2000-06-27

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

**Computerworld** - 1999-05-24

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**Security De-Engineering** - Ian Tibble 2011-12-13

As hacker organizations surpass drug cartels in terms of revenue generation, it is clear that the good guys are doing something wrong in information security. Providing a simple foundational remedy for our security ills, *Security De-Engineering: Solving the Problems in Information Risk Management* is a definitive guide to the current problems impacting corporate information risk management. It explains what the problems are, how and why they have manifested, and outlines powerful solutions. Ian Tibble delves into more than a decade of experience working with close to 100 different Fortune 500s and multinationals to explain how a gradual erosion of skills has placed corporate information assets on a disastrous collision course with automated malware attacks and manual intrusions. Presenting a complete journal of hacking feats and how corporate networks can be compromised, the book covers the most critical aspects of corporate risk information risk management. Outlines six detrimental security changes that have occurred in the past decade Examines automated vulnerability scanners and rationalizes the differences between their perceived and actual value Considers security products—including intrusion detection, security incident event management, and identity management The book provides a rare glimpse at the untold stories of what goes on behind the closed doors of private corporations. It details the tools and products that are used, typical behavioral traits, and the two types of security experts that have existed since the mid-nineties—the hackers and the consultants that came later. Answering some of the most pressing questions about network penetration testing and cloud computing security, this book provides you with the understanding and tools needed to tackle today's risk management issues as well as those on the horizon.

**Rootkits** - Greg Hoglund 2006

A guide to rootkits describes what they are, how they work, how to build them, and how to detect them.

**Computerworld** - 2000-09-11

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**Malicious Mobile Code** - Roger A. Grimes 2001-08-14

Malicious mobile code is a new term to describe all sorts of destructive programs: viruses, worms, Trojans, and

rogue Internet content. Until fairly recently, experts worried mostly about computer viruses that spread only through executable files, not data files, and certainly not through email exchange. The Melissa virus and the Love Bug proved the experts wrong, attacking Windows computers when recipients did nothing more than open an email. Today, writing programs is easier than ever, and so is writing malicious code. The idea that someone could write malicious code and spread it to 60 million computers in a matter of hours is no longer a fantasy. The good news is that there are effective ways to thwart Windows malicious code attacks, and author Roger Grimes maps them out in *Malicious Mobile Code: Virus Protection for Windows*. His opening chapter on the history of malicious code and the multi-million dollar anti-virus industry sets the stage for a comprehensive rundown on today's viruses and the nuts and bolts of protecting a system from them. He ranges through the best ways to configure Windows for maximum protection, what a DOS virus can and can't do, what today's biggest threats are, and other important and frequently surprising information. For example, how many people know that joining a chat discussion can turn one's entire computer system into an open book? *Malicious Mobile Code* delivers the strategies, tips, and tricks to secure a system against attack. It covers: The current state of the malicious code writing and cracker community How malicious code works, what types there are, and what it can and cannot do Common anti-virus defenses, including anti-virus software How malicious code affects the various Windows operating systems, and how to recognize, remove, and prevent it Macro viruses affecting MS Word, MS Excel, and VBScript Java applets and ActiveX controls Enterprise-wide malicious code protection Hoaxes The future of malicious mobile code and how to combat such code These days, when it comes to protecting both home computers and company networks against malicious code, the stakes are higher than ever. *Malicious Mobile Code* is the essential guide for securing a system from catastrophic loss.

**The Antivirus Hacker's Handbook** - Joxean Koret 2015-09-28

Hack your antivirus software to stamp out future vulnerabilities *The Antivirus Hacker's Handbook* guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus software program and work your way back through its development using the functions and other key elements of the software. Next, you leverage your new knowledge about software development to evade, attack, and exploit antivirus software—all of which can help you strengthen your network and protect your data. While not all viruses are damaging, understanding how to better protect your computer against them can help you maintain the integrity of your network. Discover how to reverse engineer your antivirus software Explore methods of antivirus software evasion Consider different ways to attack and exploit antivirus software Understand the current state of the antivirus software market, and get recommendations for users and vendors who are leveraging this software *The Antivirus Hacker's Handbook* is the essential reference for software reverse engineers, penetration testers, security researchers, exploit writers, antivirus vendors, and software engineers who want to understand how to leverage current antivirus software to improve future applications.

**Computerworld** - 2005-01-03

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**Mobile Device Security For Dummies** - Rich Campagna 2011-07-22

The information you need to avoid security threats on corporate mobile devices Mobile devices have essentially

replaced computers for corporate users who are on the go and there are millions of networks that have little to no security. This essential guide walks you through the steps for securing a network and building a bulletproof framework that will protect and support mobile devices in the enterprise. Featuring real-world case scenarios, this straightforward guide shares invaluable advice for protecting mobile devices from the loss of sensitive and confidential corporate information. Provides a practical, fast-track approach to protecting a mobile device from security threats Discusses important topics such as specific hacker protection, loss/theft protection, backing up and restoring data, and more Offers critical advice for deploying enterprise network protection for mobile devices Walks you through the advantages of granular application access control and enforcement with VPN Business can be mobile without being vulnerable?and Mobile Device Security For Dummies shows you how.

F&S Index United States Annual - 1999

*Software Development* - 2005

**Network World** - 2003-05-12

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

**Computerworld** - 2005-05-02

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

Computerworld - 2004-05-24

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

**UTM Security with Fortinet** - Kenneth Tam 2012-12-31

Traditionally, network security (firewalls to block unauthorized users, Intrusion Prevention Systems (IPS) to keep

attackers out, Web filters to avoid misuse of Internet browsing, and antivirus software to block malicious programs) required separate boxes with increased cost and complexity. Unified Threat Management (UTM) makes network security less complex, cheaper, and more effective by consolidating all these components. This book explains the advantages of using UTM and how it works, presents best practices on deployment, and is a hands-on, step-by-step guide to deploying Fortinet's FortiGate in the enterprise. Provides tips, tricks, and proven suggestions and guidelines to set up FortiGate implementations Presents topics that are not covered (or are not covered in detail) by Fortinet's documentation Discusses hands-on troubleshooting techniques at both the project deployment level and technical implementation area

- Enrico Perla 2010-10-28

A Guide to Kernel Exploitation: Attacking the Core discusses the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits, and applies them to different operating systems, namely, UNIX derivatives, Mac OS X, and Windows. Concepts and tactics are presented categorically so that even when a specifically detailed vulnerability has been patched, the foundational information provided will help hackers in writing a newer, better attack; or help pen testers, auditors, and the like develop a more concrete design and defensive structure. The book is organized into four parts. Part I introduces the kernel and sets out the theoretical basis on which to build the rest of the book. Part II focuses on different operating systems and describes exploits for them that target various bug classes. Part III on remote kernel exploitation analyzes the effects of the remote scenario and presents new techniques to target remote issues. It includes a step-by-step analysis of the development of a reliable, one-shot, remote exploit for a real vulnerabilitya bug affecting the SCTP subsystem found in the Linux kernel. Finally, Part IV wraps up the analysis on kernel exploitation and looks at what the future may hold. Covers a range of operating system families — UNIX derivatives, Mac OS X, Windows Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions Delivers the reader from user-land exploitation to the world of kernel-land (OS) exploits/attacks, with a particular focus on the steps that lead to the creation of successful techniques, in order to give to the reader something more than just a set of tricks

Computerworld - 1999-01-04

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

*A Guide to Kernel Exploitation*