

Sec760 Advanced Exploit Development For Penetration Testers 2014

Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals
 Hands on Hacking
 Python Programming for Hackers and Reverse Engineers
 Python Programming for Hackers and Pentesters
 Learning by Practicing - Mastering TShark Network Forensics
 Gray Hat Python
 Learning VMware NSX
 Ages in Chaos
 Buffer Overflow Attacks
 Windows Internals, Part 2
 Getting Started with Networking, Scripting, and Security in Kali
 From the Exodus to King Akhnaton
 A Guide to Kernel Exploitation
 Windows Internals, Part 1
 Detect, Exploit, Prevent
 The Art of Network Penetration Testing
 Offensive Countermeasures
 Black Hat Python
 The Art of Active Defense
 Kali Linux Penetration Testing Bible
 The Sculpture and Sculptors of the Greeks
 Ethical Hacking and Penetration Testing Guide
 A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
 Effective Presentations Crash Course
 Mastering Modern Web Penetration Testing
 Official (ISC)2® Guide to the CISSP®-ISSEP® CBK®
 Penetration Testing and Network Defense
 Justice Undone
 Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research
 Programming Linux Hacker Tools Uncovered: Exploits, Backdoors, Scanners, Sniffers, Brute-Forcers, Rootkits
 Clemency Decisions in the Clinton White House : Second Report
 Using Wireshark to Solve Real-world Network Problems
 A Bug Hunter's Diary
 Linux Basics for Hackers
 C Programming Absolute Beginner's Guide
 The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601)
 Go Programming For Hackers and Pentesters
 Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition
 Windows 10 System Programming, Part 1
 Discovering and Exploiting Security Holes

Sec760 Advanced Exploit Development For Penetration Testers 2014

Downloaded from archive.imba.com by guest

SCHMITT BEARD

[Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals](#) CRC Press

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

Hands on Hacking John Wiley & Sons

Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts

will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to:

- Make performant tools that can be used for your own security projects
- Create usable tools that interact with remote APIs
- Scrape arbitrary HTML data
- Use Go's standard package, net/http, for building HTTP servers
- Write your own DNS server and proxy
- Use DNS tunneling to establish a C2 channel out of a restrictive network
- Create a vulnerability fuzzer to discover an application's security weaknesses
- Use plug-ins and extensions to future-proof products
- Build an RC2 symmetric-key brute-forcer
- Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

Python Programming for Hackers and Reverse Engineers Packt Publishing Ltd
 Provides information on ways to use Wireshark to capture and analyze packets, covering such topics as building customized capture and display

filters, graphing traffic patterns, and building statistics and reports.

[Python Programming for Hackers and Pentesters](#) No Starch Press

There is nothing like the power of the kernel in Windows - but how do you write kernel drivers to take advantage of that power? This book will show you how. The book describes software kernel drivers programming for Windows. These drivers don't deal with hardware, but rather with the system itself: processes, threads, modules, registry and more. Kernel code can be used for monitoring important events, preventing some from occurring if needed. Various filters can be written that can intercept calls that a driver may be interested in.

[Learning by Practicing - Mastering TShark Network Forensics](#) БХВ-Петербург

Klein tracks down and exploits bugs in some of the world's most popular programs. Whether by browsing source code, poring over disassembly, or fuzzing live programs, readers get an over-the-shoulder glimpse into the world of a bug hunter as Klein unearths security flaws and uses them to take control of affected systems.

[Gray Hat Python](#) McGraw Hill Professional

The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks.

Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

[Learning VMware NSX](#) Microsoft Press

[CompTIA Security+ Study Guide \(Exam SY0-601\)](#)

[Ages in Chaos](#) No Starch Press

Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research is the first book available for the Metasploit Framework (MSF), which is the attack platform of choice for one of the fastest growing careers in IT security: Penetration Testing. The book will provide professional penetration testers and security researchers with a fully integrated suite of tools for discovering, running, and testing exploit code. This book discusses how to use the Metasploit Framework (MSF) as an exploitation platform. The book begins with a detailed discussion of the three MSF interfaces: msfweb, msfconsole, and msfcli. This chapter demonstrates all of the features offered by the MSF as an exploitation platform. With a solid understanding of MSF's capabilities, the book then details techniques for dramatically reducing the amount of time required for developing functional exploits. By working through a real-world vulnerabilities against popular closed source applications, the reader will learn how to use the tools and MSF to quickly build reliable attacks as standalone exploits. The section will also explain how to integrate an exploit directly into the Metasploit Framework by providing a line-by-line analysis of an integrated exploit module. Details as to how the Metasploit engine drives the behind-the-scenes exploitation process will be covered, and along the way the reader will come to understand the advantages of exploitation frameworks. The final section of the book examines the Meterpreter payload system and teaches readers to develop completely new extensions that will integrate fluidly with the Metasploit Framework. A November 2004 survey conducted by "CSO Magazine" stated that 42% of chief security officers considered penetration testing to be a security priority for their organizations The Metasploit Framework is the most popular open source exploit platform, and there are no competing books

[Buffer Overflow Attacks](#) Simon and Schuster

This much-anticipated revision, written by the ultimate group of top security experts in the world, features 40 percent new content on how to find security holes in any operating system or application New material addresses the many new exploitation techniques that have been discovered since the first edition, including attacking "unbreakable" software packages such as McAfee's Enterscept, Mac OS X, XP, Office 2003, and Vista Also features the first-ever published information on exploiting Cisco's IOS, with content that has never before been explored The companion Web site features downloadable code files

[Windows Internals, Part 2](#) Elsevier

[Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition](#) McGraw-Hill Education

[Getting Started with Networking, Scripting, and Security in Kali](#) Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: -Automate tedious reversing and security tasks -Design and program your own debugger -Learn how to fuzz Windows drivers and create powerful fuzzers from scratch -Have fun with code and network injection, soft and hard hooking techniques, and other software trickery -Sniff secure traffic out of an encrypted web browser session -Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

[From the Exodus to King Akhnaton](#) Packt Publishing Ltd

Presentation skills are the abilities an individual requires to reach a range of audiences with successful and stimulating presentations. Such abilities cover a wide range of areas such as the presentation design, the voice pitch, the slide layout, and the facial expressions one displays. A presentation is a mechanism by which an issue is presented to the public. It is typically a demonstration, introduction, lecture or speech aimed at informing,

persuading, inspiring, motivating, or building goodwill or conveying a new idea or brand. As with a maiden presentation, the concept can also be used for a formal or rhetorical introduction or proposal. Presentations are also regarded as the keynote address in certain arrangements. A presentation software is sometimes used to produce the presentation material, some of which often allow interactive production of presentations, e.g. through demographically diverse participants using the web internet. Presentation audiences can be utilized in a single presentation to integrate material from various sources. Microsoft and Apple have been offering some of the famous presentation tools used across the globe.

[A Guide to Kernel Exploitation](#) McGraw Hill Professional

The comprehensive A-to-Z guide on network security, fully revised and updated Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. If you are responsible for network security, this is the reference you need at your side. Covering new techniques, technology, and methods for approaching security, it also examines new trends and best practices being used by many organizations. The revised Network Security Bible complements the Cisco Academy course instruction in networking security. Covers all core areas of network security and how they interrelate Fully revised to address new techniques, technology, and methods for securing an enterprise worldwide Examines new trends and best practices in use by organizations to secure their enterprises Features additional chapters on areas related to data protection/correlation and forensics Includes cutting-edge topics such as integrated cybersecurity and sections on Security Landscape, with chapters on validating security, data protection, forensics, and attacks and threats If you need to get up to date or stay current on network security, Network Security Bible, 2nd Edition covers everything you need to know.

[Windows Internals, Part 1](#) Newnes

The practical guide to simulating, detecting, and responding to network attacks Create step-by-step testing plans Learn to perform social engineering and host reconnaissance Evaluate session hijacking methods Exploit web server vulnerabilities Detect attempts to breach database security Use password crackers to obtain access information Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches Scan and penetrate wireless networks Understand the inner workings of Trojan Horses, viruses, and other backdoor applications Test UNIX, Microsoft, and Novell servers for vulnerabilities Learn the root cause of buffer overflows and how to prevent them Perform and prevent Denial of Service attacks Penetration testing is a growing field but there has yet to be a definitive resource that instructs ethical hackers on how to perform a penetration test with the ethics and responsibilities of testing in mind. Penetration Testing and Network Defense offers detailed steps on how to emulate an outside attacker in order to assess the security of a network. Unlike other books on hacking, this book is specifically geared towards penetration testing. It includes important information about liability issues and ethics as well as procedures and documentation. Using popular open-source and commercial applications, the book shows you how to perform a penetration test on an organization's network, from creating a test plan to performing social engineering and host reconnaissance to performing simulated attacks on both wired and wireless networks.

Penetration Testing and Network Defense also goes a step further than other books on hacking, as it demonstrates how to detect an attack on a live network. By detailing the method of an attack and how to spot an attack on your network, this book better prepares you to guard against hackers. You will learn how to configure, record, and thwart these attacks and how to harden a system to protect it against future internal and external attacks. Full of real-world examples and step-by-step procedures, this book is both an enjoyable read and full of practical advice that will help you assess network security and develop a plan for locking down sensitive data and company resources. "This book goes to great lengths to explain the various testing approaches that are used today and gives excellent insight into how a responsible penetration testing specialist executes his trade." - Bruce Murphy, Vice President, World Wide Security Services, Cisco Systems

[Detect, Exploit, Prevent](#) John Wiley & Sons

The book is logically divided into 5 main categories with each category representing a major skill set required by most security professionals: 1. Coding - The ability to program and script is quickly becoming a mainstream requirement for just about everyone in the security industry. This section covers the basics in coding complemented with a slue of programming tips and tricks in C/C++, Java, Perl and NASL. 2. Sockets - The technology that allows programs and scripts to communicate over a network is sockets. Even though the theory remains the same - communication over TCP and UDP, sockets are implemented differently in nearly ever language. 3. Shellcode - Shellcode, commonly defined as bytecode converted from Assembly, is utilized to execute commands on remote systems via direct memory access. 4. Porting - Due to the differences between operating platforms and language implementations on those platforms, it is a common practice to modify an original body of code to work on a different platforms. This technique is known as porting and is incredible useful in the real world environments since it allows you to not "recreate the wheel. 5. Coding Tools - The culmination of the previous four sections, coding tools brings all of the techniques that you have learned to the forefront. With the background technologies and techniques you will now be able to code quick utilities that will not only make you more productive, they will arm you with an extremely valuable skill that will remain with you as long as you make the proper time and effort dedications. *Contains never before seen chapters on writing and automating exploits on windows systems with all-new exploits. *Perform zero-day exploit forensics by reverse engineering malicious code. *Provides working code and scripts in all of the most common programming languages for readers to use TODAY to defend their networks.

[The Art of Network Penetration Testing](#) John Wiley & Sons

Uncovering the development of the hacking toolset under Linux, this book teaches programmers the methodology behind hacker programming techniques so that they can think like an attacker when developing a defense. Analyses and cutting-edge programming are provided of aspects of each hacking item and its source code—including ping and traceroute utilities, viruses, worms, Trojans, backdoors, exploits (locals and remotes), scanners (CGI and port), smurf and fraggle attacks, and brute-force attacks. In addition to information on how to exploit buffer overflow errors in the stack, heap and BSS, and how to exploit format-string errors and other less common errors, this guide includes the source code of all the described utilities on the accompanying CD-ROM.

[Offensive Countermeasures](#) Amereon Limited

The book you have been waiting for to make you a Master of TShark Network Forensics, is finally here!!! Be it you are a Network Engineer, a Network Forensics Analyst, someone new to packet analysis or someone who occasionally looks at packet, this book is guaranteed to improve your TShark

skills, while moving you from Zero to Hero. Mastering TShark Network Forensics, can be considered the definitive repository of practical TShark knowledge. It is your one-stop shop for all you need to master TShark, with adequate references to allow you to go deeper on peripheral topics if you so choose. Book Objectives: Introduce packet capturing architecture Teach the basics of TShark Teach some not so basic TShark tricks Solve real world challenges with TShark Identify services hiding behind other protocols Perform "hands-free" packet capture with TShark Analyze and decrypt TLS encrypted traffic Analyze and decrypt WPA2 Personal Traffic Going way beyond - Leveraging TShark and Python for IP threat intelligence Introduce Lua scripts Introduce packet editing Introduce packet merging Introduce packet rewriting Introduce remote packet capturing Who is this book for? While this book is written specifically for Network Forensics Analysts, it is equally beneficial to anyone who supports the network infrastructure. This means, Network Administrators, Security Specialists, Network Engineers, etc., will all benefit from this book. Considering the preceding, I believe the following represents the right audience for this book: Individuals starting off their Cybersecurity careers Individuals working in a Cyber/Security Operations Center (C/SOC) General practitioners of Cybersecurity Experienced Cybersecurity Ninjas who may be looking for a trick or two Anyone who just wishes to learn more about TShark and its uses in network forensics Anyone involved in network forensics More importantly, anyhow who is looking for a good read Not sure if this book is for you? Take a glimpse at the sample chapter before committing to it. Mastering TShark sample chapters can be found at: <https://bit.ly/TShark> All PCAPS used within this book can be found at: <https://github.com/SecurityNik/SUWtHEh> As an addition to this book, the tool, pktIntel: Tool used to perform threat intelligence against packet data can be found at: <https://github.com/SecurityNik/pktIntel>

Black Hat Python Paradigma Ltd

The definitive guide-fully updated for Windows 10 and Windows Server 2016 Delve inside Windows architecture and internals, and see how core components work behind the scenes. Led by a team of internals experts, this classic guide has been fully updated for Windows 10 and Windows Server 2016. Whether you are a developer or an IT professional, you'll get critical, insider perspectives on how Windows operates. And through hands-on experiments, you'll experience its internal behavior firsthand-knowledge you can apply to improve application design, debugging, system performance, and support. This book will help you: · Understand the Window system architecture and its most important entities, such as processes and threads · Examine how processes manage resources and threads scheduled for execution inside processes · Observe how Windows manages virtual and physical memory · Dig into the Windows I/O system and see how device drivers work and integrate with the rest of the system · Go inside the Windows security model to see how it manages access, auditing, and authorization, and learn about the new mechanisms in Windows 10 and

Related with Sec760 Advanced Exploit Development For Penetration Testers 2014:

- Onsc Oncology Chemotherapy Immunotherapy Certificate Test Answers : [click here](#)

Server 2016

The Art of Active Defense John Wiley & Sons

Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does! About This Book This book covers the latest technologies such as Advance XSS, XSRF, SQL Injection, Web API testing, XML attack vectors, OAuth 2.0 Security, and more involved in today's web applications Penetrate and secure your web application using various techniques Get this comprehensive reference guide that provides advanced tricks and tools of the trade for seasoned penetration testers Who This Book Is For This book is for security professionals and penetration testers who want to speed up their modern web application penetrating testing. It will also benefit those at an intermediate level and web developers who need to be aware of the latest application hacking techniques. What You Will Learn Get to know the new and less-publicized techniques such PHP Object Injection and XML-based vectors Work with different security tools to automate most of the redundant tasks See different kinds of newly-designed security headers and how they help to provide security Exploit and detect different kinds of XSS vulnerabilities Protect your web application using filtering mechanisms Understand old school and classic web hacking in depth using SQL Injection, XSS, and CSRF Grasp XML-related vulnerabilities and attack vectors such as XXE and DoS techniques Get to know how to test REST APIs to discover security issues in them In Detail Web penetration testing is a growing, fast-moving, and absolutely critical field in information security. This book executes modern web application attacks and utilises cutting-edge hacking techniques with an enhanced knowledge of web application security. We will cover web hacking techniques so you can explore the attack vectors during penetration tests. The book encompasses the latest technologies such as OAuth 2.0, Web API testing methodologies and XML vectors used by hackers. Some lesser discussed attack vectors such as RPO (relative path overwrite), DOM clobbering, PHP Object Injection and etc. has been covered in this book. We'll explain various old school techniques in depth such as XSS, CSRF, SQL Injection through the ever-dependable SQLMap and reconnaissance. Websites nowadays provide APIs to allow integration with third party applications, thereby exposing a lot of attack surface, we cover testing of these APIs using real-life examples. This pragmatic guide will be a great benefit and will help you prepare fully secure applications. Style and approach This master-level guide covers various techniques serially. It is power-packed with real-world examples that focus more on the practical aspects of implementing the techniques rather going into detailed theory.

Kali Linux Penetration Testing Bible McGraw-Hill Education

Delve into programming the Windows operating system through the Windows API in with C++. Use the power of the Windows API to working with processes, threads, jobs, memory, I/O and more. The book covers current Windows 10 versions, allowing you to get the most of what Windows has to offer to developers in terms of productivity, performance and scalability.