Malware Forensics Field Guide For Linux Systems

#Malware Forensics #Linux Systems #Incident Response #Digital Forensics #Linux Malware Analysis

This guide provides a practical approach to malware forensics on Linux systems. It covers key techniques for identifying, analyzing, and mitigating malware threats, making it an essential resource for security professionals and incident responders dealing with compromised Linux environments. Learn how to effectively investigate and respond to malware incidents, enhancing your organization's security posture and minimizing potential damage from cyberattacks on Linux based systems.

Malware Forensics Field Guide for Linux Systems

Malware Forensics Field Guide for Linux Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program. This book will appeal to computer forensic investigators, analysts, and specialists. A compendium of on-the-job tasks and checklists Specific for Linux-based systems in which new malware is developed every day Authors are world-renowned leaders in investigating and analyzing malicious code

Linux Malware Incident Response: A Practitioner's Guide to Forensic Collection and Examination of Volatile Data

Linux Malware Incident Response is a "first look" at the Malware Forensics Field Guide for Linux Systems, exhibiting the first steps in investigating Linux-based incidents. The Syngress Digital Forensics Field Guides series includes companions for any digital and computer forensic investigator and analyst. Each book is a "toolkit" with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. This compendium of tools for computer forensics analysts and investigators is presented

in a succinct outline format with cross-references to supplemental appendices. It is designed to provide the digital investigator clear and concise guidance in an easily accessible format for responding to an incident or conducting analysis in a lab. Presented in a succinct outline format with cross-references to included supplemental components and appendices Covers volatile data collection methodology as well as non-volatile data collection from a live Linux system Addresses malware artifact discovery and extraction from a live Linux system

Malware Forensics Field Guide for Windows Systems

Malware Forensics Field Guide for Windows Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Windows-based systems, the largest running OS in the world. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Windows system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Windows systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Windows system; and analysis of a suspect program. This field guide is intended for computer forensic investigators, analysts, and specialists. A condensed hand-held guide complete with on-the-job tasks and checklists Specific for Windows-based systems, the largest running OS in the world Authors are world-renowned leaders in investigating and analyzing malicious code

Malware Forensics

Malware Forensics: Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system. It is the first book detailing how to perform live forensic techniques on malicious code. The book gives deep coverage on the tools and techniques of conducting runtime behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more. It explores over 150 different tools for malware incident response and analysis, including forensic tools for preserving and analyzing computer memory. Readers from all educational and technical backgrounds will benefit from the clear and concise explanations of the applicable legal case law and statutes covered in every chapter. In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter. This book is intended for system administrators, information security professionals, network personnel, forensic examiners, attorneys, and law enforcement working with the inner-workings of computer memory and malicious code. * Winner of Best Book Bejtlich read in 2008! * http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html * Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader. * First book to detail how to perform "live forensic" techniques on malicous code. * In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

The Art of Memory Forensics

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring

you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

Practical Malware Analysis

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: –Set up a safe virtual environment to analyze malware –Quickly extract network signatures and host-based indicators –Use key analysis tools like IDA Pro, OllyDbg, and WinDbg –Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques –Use your newfound knowledge of Windows internals for malware analysis –Develop a methodology for unpacking malware and get practical experience with five of the most popular packers –Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

UNIX and Linux Forensic Analysis DVD Toolkit

This book addresses topics in the area of forensic analysis of systems running on variants of the UNIX operating system, which is the choice of hackers for their attack platforms. According to a 2007 IDC report, UNIX servers account for the second-largest segment of spending (behind Windows) in the worldwide server market with $4.2 billion in 2Q07, representing 31.7% of corporate server spending. UNIX systems have not been analyzed to any significant depth largely due to a lack of understanding on the part of the investigator, an understanding and knowledge base that has been achieved by the attacker. The book begins with a chapter to describe why and how the book was written, and for whom, and then immediately begins addressing the issues of live response (volatile) data collection and analysis. The book continues by addressing issues of collecting and analyzing the contents of physical memory (i.e., RAM). The following chapters address /proc analysis, revealing the wealth of significant evidence, and analysis of files created by or on UNIX systems. Then the book addresses the underground world of UNIX hacking and reveals methods and techniques used by hackers, malware coders, and anti-forensic developers. The book then illustrates to the investigator how to analyze these files and extract the information they need to perform a comprehensive forensic analysis. The final chapter includes a detailed discussion of loadable kernel Modules and malware. Throughout the book the author provides a wealth of unique information, providing tools, techniques and information that won't be found anywhere else. This book contains information about UNIX forensic analysis that is not available anywhere else. Much of the information is a result of the author's own unique research and work. The authors have the combined experience of law enforcement, military, and corporate forensics. This unique perspective makes this book attractive to all forensic investigators.

Practical Linux Forensics

A resource to help forensic investigators locate, analyze, and understand digital evidence found on modern Linux systems after a crime, security incident or cyber attack. Practical Linux Forensics dives into the technical details of analyzing postmortem forensic images of Linux systems which have been misused, abused, or the target of malicious attacks. It helps forensic investigators locate and analyze digital evidence found on Linux desktops, servers, and IoT devices. Throughout the book, you learn how to identify digital artifacts which may be of interest to an investigation, draw logical conclusions, and reconstruct past activity from incidents. You'll learn how Linux works from a digital forensics and investigation perspective, and how to interpret evidence from Linux environments. The techniques shown are intended to be independent of the forensic analysis platforms and tools used. Learn how to: Extract evidence from storage devices and analyze partition tables, volume managers, popular Linux filesystems (Ext4, Btrfs, and Xfs), and encryption Investigate evidence from Linux logs, including traditional syslog, the systemd journal, kernel and audit logs, and logs from daemons and applications Reconstruct the Linux startup process, from boot loaders (UEFI and Grub) and kernel initialization, to systemd unit files and targets leading up to a graphical login Perform analysis of power, temperature, and the physical environment of a Linux machine, and find evidence of sleep, hibernation, shutdowns, reboots, and crashes Examine installed software, including distro installers, package formats, and package management systems from Debian, Fedora, SUSE, Arch, and other distros Perform analysis of time and Locale settings, internationalization including language and keyboard settings, and geolocation on a Linux system Reconstruct user login sessions (shell, X11 and Wayland), desktops (Gnome, KDE, and others) and analyze keyrings, wallets, trash cans, clipboards, thumbnails, recent files and other desktop artifacts Analyze network configuration, including interfaces, addresses, network managers, DNS, wireless artifacts (Wi-Fi, Bluetooth, WWAN), VPNs (including WireGuard), firewalls, and proxy settings Identify traces of attached peripheral devices (PCI, USB, Thunderbolt, Bluetooth) including external storage, cameras, and mobiles, and reconstruct printing and scanning activity

Digital Forensics with Open Source Tools

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems

Windows Registry Forensics

Windows Registry Forensics provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques are presented that take the student and analyst beyond the current use of viewers and into real analysis of data contained in the Registry, demonstrating the forensic value of the Registry. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this book is packed with real-world examples using freely available open source tools. It also includes case studies and a CD containing code and author-created tools discussed in the book. This book will appeal to computer forensic and incident response professionals, including federal government and commercial/private sector contractors, consultants, etc. Named a 2011 Best Digital Forensics Book by InfoSec Reviews Packed with real-world examples using freely available open source tools Deep explanation and understanding of the Windows Registry – the most difficult part of Windows to analyze forensically Includes a CD containing code and author-created tools discussed in the book

Operating System Forensics

Operating System Forensics is the first book to cover all three critical operating systems for digital forensic investigations in one comprehensive reference. Users will learn how to conduct successful digital forensic examinations in Windows, Linux, and Mac OS, the methodologies used, key technical concepts, and the tools needed to perform examinations. Mobile operating systems such as Android, iOS, Windows, and Blackberry are also covered, providing everything practitioners need to conduct a forensic investigation of the most commonly used operating systems, including technical details of how each operating system works and how to find artifacts. This book walks you through the critical components of investigation and operating system functionality, including file systems, data recovery, memory forensics, system configuration, Internet access, cloud computing, tracking artifacts, executable layouts, malware, and log files. You'll find coverage of key technical topics like Windows Registry, /etc directory, Web browers caches, Mbox, PST files, GPS data, ELF, and more. Hands-on exercises in each chapter drive home the concepts covered in the book. You'll get everything you need for a successful forensics examination, including incident response tactics and legal requirements. Operating System Forensics is the only place you'll find all this covered in one book. Covers digital forensic investigations of the three major operating systems, including Windows, Linux, and Mac OS Presents the technical details of each operating system, allowing users to find artifacts that might be missed using automated tools Hands-on exercises drive home key concepts covered in the book. Includes discussions of cloud, Internet, and major mobile operating systems such as Android and iOS

Digital Forensics Basics

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigationsGather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10–specific feature forensicsUtilize anti-forensic techniques, including steganography, data destruction techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals

File System Forensic Analysis

The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Most digital evidence is stored within the computer's file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed. Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today's most valuable open source file system analysis tools—including tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk's Host Protected Area (HPA) Reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more Analyzing DOS, Apple,

and GPT partitions; BSD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques Analyzing the contents of multiple disk volumes, such as RAID and disk spanning Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools When it comes to file system analysis, no other book offers this much detail or expertise. Whether you're a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist, or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use.

Learning Malware Analysis

Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you’ll be able to get most out of this book.

Nikon D5300 Digital Field Guide

Everything you need to know to take amazing photographs using your new DSLR The Nikon D5300 Digital Field Guide is filled with everything you need to know to take fantastic photos with your new Nikon. In full color, this portable guide covers all of the essential controls, features, and functions of the Nikon D5300, using step-by-step instructions and providing full-color images of each menu screen. Nikon users will love this comprehensive field guide—it's just the right size to fit into a camera bag, so you'll be able to take it wherever your photography adventures take you. The guide goes beyond camera settings, offering you a refresher course in digital photography principles, and covering the essentials of lighting, composition, and exposure. This perfectly sized field guide features: Compact size, allowing photographers to carry it wherever they go Professional advice on everything from composing a variety of shots to choosing lenses Colorful example images, along with detailed instructions on how to get the most from each of the camera's features Filled with amazing examples, this handy guide offers a variety of tips and tricks. You'll learn how to capture portraits, take character-filled candid shots, frame sports action, document travel, work with macro photography, and much more!

Security Warrior

When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm.What's the worst an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your

attacker in depth, Security Warrior reveals how your systems can be attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antiforensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle.Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability.Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands.

Canon EOS 7D Digital Field Guide

No-fail formulas for getting great digital photos with the Canon EOS 7D If you want to polish your photography skills, keep your camera bag stocked with the best equipment, like Canon's new EOS 7D camera and this practical, full-color Canon EOS 7D Digital Field Guide. Portable and packed with information, this handy guide helps you get the very most out of the EOS 7D's powerful new features. Discover professional shooting tricks, helpful composition advice, and invaluable tips on exposure, perspective, and more. The book also includes a grey and color checker card, so you can tweak your captured photos for optimal colorization. From menu screens to composition, this book provides no-fail techniques for getting the most out of your Canon EOS 7D digital camera Covers the camera's new features, including the 19-point autofocus, new metering system, integrated Speedlight Transmitter, 8-frames-per-second shooting ratio, and improved HD video capturing Helps you take your photography skills to another level with photography tips and tricks from professional photographer and author Charlotte Lowrie Teaches you photography essentials such as composition, exposure, perspective, and more Includes a grey and color card checker and full instructions with the book Take memorable photographs with your new Canon EOS 7D and the Canon EOS 7D Digital Field Guide!

Mastering Malware Analysis

Master malware analysis to protect your systems from getting infected Key FeaturesSet up and model solutions, investigate malware, and prevent it from occurring in futureLearn core concepts of dynamic malware analysis, memory forensics, decryption, and much moreA practical guide to developing innovative solutions to numerous malware incidentsBook Description With the ever-growing proliferation of technology, the risk of encountering malicious code or malware has also increased. Malware analysis has become one of the most trending topics in businesses in recent years due to multiple prominent ransomware attacks. Mastering Malware Analysis explains the universal patterns behind different malicious software types and how to analyze them using a variety of approaches. You will learn how to examine malware code and determine the damage it can possibly cause to your systems to ensure that it won't propagate any further. Moving forward, you will cover all aspects of malware analysis for the Windows platform in detail. Next, you will get to grips with obfuscation and anti-disassembly, anti-debugging, as well as anti-virtual machine techniques. This book will help you deal with modern cross-platform malware. Throughout the course of this book, you will explore real-world examples of static and dynamic malware analysis, unpacking and decrypting, and rootkit detection. Finally, this book will help you strengthen your defenses and prevent malware breaches for IoT devices and mobile platforms. By the end of this book, you will have learned to effectively analyze, investigate, and build innovative solutions to handle any malware incidents. What you will learnExplore widely used assembly languages to strengthen your reverse-engineering skillsMaster different executable file formats, programming languages, and relevant APIs used by attackersPerform static and dynamic analysis for multiple platforms and file typesGet to grips with handling sophisticated malware casesUnderstand real advanced attacks, covering all stages from infiltration to hacking the systemLearn to bypass anti-reverse engineering techniquesWho this book is for If you are an IT security administrator, forensic analyst, or malware researcher looking to secure against malicious software or investigate malicious code, this book is for you. Prior programming experience and a fair understanding of malware attacks and investigation is expected.

Digital Evidence and Computer Crime

Though an increasing number of criminals are using computers and computer networks, few investigators are well versed in the issues related to digital evidence. This work explains how computer networks function and how they can be used in a crime.

Practical Memory Forensics

A practical guide to enhancing your digital investigations with cutting-edge memory forensics techniques Key FeaturesExplore memory forensics, one of the vital branches of digital investigationLearn the art of user activities reconstruction and malware detection using volatile memoryGet acquainted with a range of open-source tools and techniques for memory forensicsBook Description Memory Forensics is a powerful analysis technique that can be used in different areas, from incident response to malware analysis. With memory forensics, you can not only gain key insights into the user's context but also look for unique traces of malware, in some cases, to piece together the puzzle of a sophisticated targeted attack. Starting with an introduction to memory forensics, this book will gradually take you through more modern concepts of hunting and investigating advanced malware using free tools and memory analysis frameworks. This book takes a practical approach and uses memory images from real incidents to help you gain a better understanding of the subject and develop the skills required to investigate and respond to malware-related incidents and complex targeted attacks. You'll cover Windows, Linux, and macOS internals and explore techniques and tools to detect, investigate, and hunt threats using memory forensics. Equipped with this knowledge, you'll be able to create and analyze memory dumps on your own, examine user activity, detect traces of fileless and memory-based malware, and reconstruct the actions taken by threat actors. By the end of this book, you'll be well-versed in memory forensics and have gained hands-on experience of using various tools associated with it. What you will learnUnderstand the fundamental concepts of memory organizationDiscover how to perform a forensic investigation of random access memoryCreate full memory dumps as well as dumps of individual processes in Windows, Linux, and macOSAnalyze hibernation files, swap files, and crash dumpsApply various methods to analyze user activitiesUse multiple approaches to search for traces of malicious activityReconstruct threat actor tactics and techniques using random access memory analysisWho this book is for This book is for incident responders, digital forensic specialists, cybersecurity analysts, system administrators, malware analysts, students, and curious security professionals new to this field and interested in learning memory forensics. A basic understanding of malware and its working is expected. Although not mandatory, knowledge of operating systems internals will be helpful. For those new to this field, the book covers all the necessary concepts.

Malware Analyst's Cookbook and DVD

A computer forensics "how-to" for fighting malicious code andanalyzing incidents With our ever-increasing reliance on computers comes anever-growing risk of malware. Security professionals will findplenty of solutions in this book to the problems posed by viruses,Trojan horses, worms, spyware, rootkits, adware, and other invasivesoftware. Written by well-known malware experts, this guide revealssolutions to numerous problems and includes a DVD of customprograms and tools that illustrate the concepts, enhancing yourskills. Security professionals face a constant battle against malicioussoftware; this practical manual will improve your analyticalcapabilities and provide dozens of valuable and innovativesolutions Covers classifying malware, packing and unpacking, dynamicmalware analysis, decoding and decrypting, rootkit detection,memory forensics, open source malware research, and much more Includes generous amounts of source code in C, Python, and Perlto extend your favorite tools or build new ones, and customprograms on the DVD to demonstrate the solutions Malware Analyst's Cookbook is indispensible to ITsecurity administrators, incident responders, forensic analysts,and malware researchers.

Linux Forensics

Linux Forensics is the most comprehensive and up-to-date resource for those wishing to quickly and efficiently perform forensicson Linux systems. It is also a great asset for anyone that would like to better understand Linux internals. Linux Forensics will guide you step by step through the process of investigating a computer running Linux. Everything you need to know from the moment you receive the call from someone who thinks they have been attacked until the final report is written is covered in this book. All of the tools discussed in this book are free and most are also open source. Dr. Philip Polstra shows how to leverage numerous tools such as Python, shell scripting, and MySQL to quickly, easily, and accurately analyze Linux systems. While readers will have a strong grasp

of Python and shell scripting by the time they complete this book, no priorknowledge of either of these scripting languages is assumed. Linux Forensics begins by showing you how to determine if there was an incident with minimally invasive techniques. Once it appears likely that an incident has occurred, Dr. Polstra shows you how to collect data from a live system before shutting it down for the creation of filesystem images. Linux Forensics contains extensive coverage of Linux ext2, ext3, and ext4 filesystems. A large collection of Python and shell scripts for creating, mounting, and analyzing filesystem images are presented in this book. Dr. Polstra introduces readers to the exciting new field of memory analysis using the Volatility framework. Discussions of advanced attacks and malware analysis round out the book. Book Highlights 370 pages in large, easy-to-read 8.5 x 11 inch format Over 9000 lines of Python scripts with explanations Over 800 lines of shell scripts with explanations A 102 page chapter containing up-to-date information on the ext4 filesystem Two scenarios described in detail with images available from the book website All scripts and other support files are available from the book website Chapter Contents First Steps General Principles Phases of Investigation High-level Process Building a Toolkit Determining If There Was an Incident Opening a Case Talking to Users Documenation Mounting Known-good Binaries Minimizing Disturbance to the Subject Automation With Scripting Live Analysis Getting Metadata Using Spreadsheets Getting Command Histories Getting Logs Using Hashes Dumping RAM Creating Images Shutting Down the System Image Formats DD DCFLDD Write Blocking Imaging Virtual Machines Imaging Physical Drives Mounting Images Master Boot Record Based Partions GUID Partition Tables Mounting Partitions In Linux Automating With Python Analyzing Mounted Images Getting Timestamps Using LibreOffice Using MySQL Creating Timelines Extended Filesystems Basics Superblocks Features Using Python Finding Things That Are Out Of Place Inodes Journaling Memory Analysis Volatility Creating Profiles Linux Commands Dealing With More Advanced Attackers Malware Is It Malware? Malware Analysis Tools Static Analysis Dynamic Analysis Obfuscation The Road Ahead Learning More Communities Conferences Certifications

Rootkits and Bootkits

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.

Cuckoo Malware Analysis

This book is a step-by-step, practical tutorial for analyzing and detecting malware and performing digital investigations. This book features clear and concise guidance in an easily accessible format.Cuckoo Malware Analysis is great for anyone who wants to analyze malware through programming, networking, disassembling, forensics, and virtualization. Whether you are new to malware analysis or have some experience, this book will help you get started with Cuckoo Sandbox so you can start analysing malware effectively and efficiently.

Windows Forensic Analysis DVD Toolkit

Windows Forensic Analysis DVD Toolkit, 2nd Edition, is a completely updated and expanded version of Harlan Carvey's best-selling forensics book on incident response and investigating cybercrime on Windows systems. With this book, you will learn how to analyze data during live and post-mortem investigations. New to this edition is Forensic Analysis on a Budget, which collects freely available tools that are essential for small labs, state (or below) law enforcement, and educational organizations.

The book also includes new pedagogical elements, Lessons from the Field, Case Studies, and War Stories that present real-life experiences by an expert in the trenches, making the material real and showing the why behind the how. The companion DVD contains significant, and unique, materials (movies, spreadsheet, code, etc.) not available anyplace else because they were created by the author. This book will appeal to digital forensic investigators, IT security professionals, engineers, and system administrators as well as students and consultants. Best-Selling Windows Digital Forensic book completely updated in this 2nd Edition Learn how to Analyze Data During Live and Post-Mortem Investigations DVD Includes Custom Tools, Updated Code, Movies, and Spreadsheets!

Digital Forensics with Kali Linux

Learn the skills you need to take advantage of Kali Linux for digital forensics investigations using this comprehensive guide About This Book Master powerful Kali Linux tools for digital investigation and analysis Perform evidence acquisition, preservation, and analysis using various tools within Kali Linux Implement the concept of cryptographic hashing and imaging using Kali Linux Perform memory forensics with Volatility and internet forensics with Xplico. Discover the capabilities of professional forensic tools such as Autopsy and DFF (Digital Forensic Framework) used by law enforcement and military personnel alike Who This Book Is For This book is targeted at forensics and digital investigators, security analysts, or any stakeholder interested in learning digital forensics using Kali Linux. Basic knowledge of Kali Linux will be an advantage. What You Will Learn Get to grips with the fundamentals of digital forensics and explore best practices Understand the workings of file systems, storage, and data fundamentals Discover incident response procedures and best practices Use DC3DD and Guymager for acquisition and preservation techniques Recover deleted data with Foremost and Scalpel Find evidence of accessed programs and malicious programs using Volatility. Perform network and internet capture analysis with Xplico Carry out professional digital forensics investigations using the DFF and Autopsy automated forensic suites In Detail Kali Linux is a Linux-based distribution used mainly for penetration testing and digital forensics. It has a wide range of tools to help in forensics investigations and incident response mechanisms. You will start by understanding the fundamentals of digital forensics and setting up your Kali Linux environment to perform different investigation practices. The book will delve into the realm of operating systems and the various formats for file storage, including secret hiding places unseen by the end user or even the operating system. The book will also teach you to create forensic images of data and maintain integrity using hashing tools. Next, you will also master some advanced topics such as autopsies and acquiring investigation data from the network, operating system memory, and so on. The book introduces you to powerful tools that will take your forensic abilities and investigations to a professional level, catering for all aspects of full digital forensic investigations from hashing to reporting. By the end of this book, you will have had hands-on experience in implementing all the pillars of digital forensics—acquisition, extraction, analysis, and presentation using Kali Linux tools. Style and approach While covering the best practices of digital forensics investigations, evidence acquisition, preservation, and analysis, this book delivers easy-to-follow practical examples and detailed labs for an easy approach to learning forensics. Following the guidelines within each lab, you can easily practice all readily available forensic tools in Kali Linux, within either a dedicated physical or virtual machine.

Handbook of Digital Forensics and Investigation

Handbook of Digital Forensics and Investigation builds on the success of the Handbook of Computer Crime Investigation, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is also designed as an accompanying text to Digital Evidence and Computer Crime. This unique collection details how to conduct digital investigations in both criminal and civil contexts, and how to locate and utilize digital evidence on computers, networks, and embedded systems. Specifically, the Investigative Methodology section of the Handbook provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery, and Intrusion Investigation. The Technology section is extended and updated to reflect the state of the art in each area of specialization. The main areas of focus in the Technology section are forensic analysis of Windows, Unix, Macintosh, and embedded systems (including cellular telephones and other mobile devices), and investigations involving networks (including enterprise environments and mobile telecommunications technology). This handbook is an essential technical reference and on-the-job guide that IT professionals, forensic practitioners, law enforcement, and attorneys will rely on when confronted with computer related crime and digital evidence of any kind. *Provides methodologies proven in practice for conducting digital investigations of all kinds

*Demonstrates how to locate and interpret a wide variety of digital evidence, and how it can be useful in investigations *Presents tools in the context of the investigative process, including EnCase, FTK, ProDiscover, foremost, XACT, Network Miner, Splunk, flow-tools, and many other specialized utilities and analysis platforms *Case examples in every chapter give readers a practical understanding of the technical, logistical, and legal challenges that arise in real investigations

Practical Forensic Imaging

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. Practical Forensic Imaging takes a detailed look at how to secure and manage digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: –Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies –Protect attached evidence media from accidental modification –Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal –Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping –Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt –Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OS-encrypted drives using BitLocker, FileVault, and TrueCrypt; and others –Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, Practical Forensic Imaging is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab.

Real digital forensics

Stop manually analyzing binary! Practical Binary Analysis is the first book of its kind to present advanced binary analysis topics, such as binary instrumentation, dynamic taint analysis, and symbolic execution, in an accessible way. As malware increasingly obfuscates itself and applies anti-analysis techniques to thwart our analysis, we need more sophisticated methods that allow us to raise that dark curtain designed to keep us out--binary analysis can help. The goal of all binary analysis is to determine (and possibly modify) the true properties of binary programs to understand what they really do, rather than what we think they should do. While reverse engineering and disassembly are critical first steps in many forms of binary analysis, there is much more to be learned. This hands-on guide teaches you how to tackle the fascinating but challenging topics of binary analysis and instrumentation and helps you become proficient in an area typically only mastered by a small group of expert hackers. It will take you from basic concepts to state-of-the-art methods as you dig into topics like code injection, disassembly, dynamic taint analysis, and binary instrumentation. Written for security engineers, hackers, and those with a basic working knowledge of C/C++ and x86-64, Practical Binary Analysis will teach you in-depth how binary programs work and help you acquire the tools and techniques needed to gain more control and insight into binary programs. Once you've completed an introduction to basic binary formats, you'll learn how to analyze binaries using techniques like the GNU/Linux binary analysis toolchain, disassembly, and code injection. You'll then go on to implement profiling tools with Pin and learn how to build your own dynamic taint analysis tools with libdft and symbolic execution tools using Triton. You'll learn how to: - Parse ELF and PE binaries and build a binary loader with libbfd - Use data-flow analysis techniques like program tracing, slicing, and reaching definitions analysis to reason about runtime flow of your programs - Modify ELF binaries with techniques like parasitic code injection and hex editing - Build custom disassembly tools with Capstone - Use binary instrumentation to circumvent anti-analysis tricks commonly used by malware - Apply taint analysis to detect control hijacking and data leak attacks - Use symbolic execution to build automatic exploitation tools With exercises at the end of each chapter to help solidify your skills, you'll go from understanding basic assembly to performing some of the most sophisticated binary analysis and instrumentation. Practical Binary Analysis gives you what you need to work effectively with binary programs and transform your knowledge from basic understanding to expert-level proficiency.

Practical Binary Analysis

Easy-to-understand techniques for getting the most from your Canon EOS 5D Mark II DSLR At nearly $3,000 for the body only, the Canon 5D Mark II DSLR is for amateurs and semi-professionals who are serious about taking great photos-and this go-anywhere guide shares insight for doing just that. Authors Charlotte Lowrie and Brian McLernon walk you step by step through each function on the Canon EOS 5D Mark II, going into more depth and scope than the standard manual that accompanies the camera. Portable and easy to understand, the book shows you how to get the exact show you want, when you want them, and is packed with more than 200 beautiful color photos. Includes step-by-step techniques and professional tips on taking exceptional photos with your Canon EOS 5D Mark II Reviews how to better understand the various functions and potential of your Canon EOS 5D Mark II Features samples of inspirational photos taken by the author With so much helpful advice for getting the most out of your Canon EOS 5D Mark II, you'll be referencing this guide again and again.

Canon EOS 5D Mark II Digital Field Guide

The rapid growth and development of Android-based devices has resulted in a wealth of sensitive information on mobile devices that offer minimal malware protection. This has created an immediate need for security professionals that understand how to best approach the subject of Android malware threats and analysis.In Android Malware and Analysis, K

Android Malware and Analysis

Become an effective cyber forensics investigator and gain a collection of practical, efficient techniques to get the job done. Diving straight into a discussion of anti-forensic techniques, this book shows you the many ways to effectively detect them. Now that you know what you are looking for, you'll shift your focus to network forensics, where you cover the various tools available to make your network forensics process less complicated. Following this, you will work with cloud and mobile forensic techniques by considering the concept of forensics as a service (FaSS), giving you cutting-edge skills that will future-proof your career. Building on this, you will learn the process of breaking down malware attacks, web attacks, and email scams with case studies to give you a clearer view of the techniques to be followed. Another tricky technique is SSD forensics, so the author covers this in detail to give you the alternative analysis techniques you'll need. To keep you up to speed on contemporary forensics, Practical Cyber Forensics includes a chapter on Bitcoin forensics, where key crypto-currency forensic techniques will be shared. Finally, you will see how to prepare accurate investigative reports. What You Will LearnCarry out forensic investigation on Windows, Linux, and macOS systems Detect and counter anti-forensic techniques Deploy network, cloud, and mobile forensics Investigate web and malware attacks Write efficient investigative reports Who This Book Is For Intermediate infosec professionals looking for a practical approach to investigative cyber forensics techniques.

Practical Cyber Forensics

"Don"t look now, but your fingerprints are all over the cover of this book. Simply picking it up off the shelf to read the cover has left a trail of evidence that you were here. "If you think book covers are bad, computers are worse. Every time you use a computer, you leave elephant-sized tracks all over it. As Dan and Wietse show, even people trying to be sneaky leave evidence all over, sometimes in surprising places. "This book is about computer archeology. It"s about finding out what might have been based on what is left behind. So pick up a tool and dig in. There"s plenty to learn from these masters of computer security." --Gary McGraw, Ph.D., CTO, Cigital, coauthor of Exploiting Software and Building Secure Software "A wonderful book. Beyond its obvious uses, it also teaches a great deal about operating system internals." --Steve Bellovin, coauthor of Firewalls and Internet Security, Second Edition, and Columbia University professor "A must-have reference book for anyone doing computer forensics. Dan and Wietse have done an excellent job of taking the guesswork out of a difficult topic." --Brad Powell, chief security architect, Sun Microsystems, Inc. "Farmer and Venema provide the essential guide to "fossil" data. Not only do they clearly describe what you can find during a forensic investigation, they also provide research found nowhere else about how long data remains on disk and in memory. If you ever expect to look at an exploited system, I highly recommend reading this book." --Rik Farrow, Consultant, author of Internet Security for Home and Office "Farmer and Venema do for digital archaeology what Indiana Jones did for historical archaeology. Forensic Discovery unearths hidden treasures in enlightening and entertaining ways, showing how a time-centric approach to computer forensics reveals even the cleverest intruder." --Richard Bejtlich, technical director, ManTech

CFIA, and author of The Tao of Network Security Monitoring "Farmer and Venema are "hackers" of the old school: They delight in understanding computers at every level and finding new ways to apply existing information and tools to the solution of complex problems." --Muffy Barkocy, Senior Web Developer, Shopping.com "This book presents digital forensics from a unique perspective because it examines the systems that create digital evidence in addition to the techniques used to find it. I would recommend this book to anyone interested in learning more about digital evidence from UNIX systems." --Brian Carrier, digital forensics researcher, and author of File System Forensic Analysis The Definitive Guide to Computer Forensics: Theory and Hands-On Practice Computer forensics--the art and science of gathering and analyzing digital evidence, reconstructing data and attacks, and tracking perpetrators--is becoming ever more important as IT and law enforcement professionals face an epidemic in computer crime. In Forensic Discovery, two internationally recognized experts present a thorough and realistic guide to the subject. Dan Farmer and Wietse Venema cover both theory and hands-on practice, introducing a powerful approach that can often recover evidence considered lost forever. The authors draw on their extensive firsthand experience to cover everything from file systems, to memory and kernel hacks, to malware. They expose a wide variety of computer forensics myths that often stand in the way of success. Readers will find extensive examples from Solaris, FreeBSD, Linux, and Microsoft Windows, as well as practical guidance for writing one"s own forensic tools. The authors are singularly well-qualified to write this book: They personally created some of the most popular security tools ever written, from the legendary SATAN network scanner to the powerful Coroner"s Toolkit for analyzing UNIX break-ins. After reading this book you will be able to Understand essential forensics concepts: volatility, layering, and trust Gather the maximum amount of reliable evidence from a running system Recover partially destroyed information--and make sense of it Timeline your system: understand what really happened when Uncover secret changes to everything from system utilities to kernel modules Avoid cover-ups and evidence traps set by intruders Identify the digital footprints associated with suspicious activity Understand file systems from a forensic analyst"s point of view Analyze malware--without giving it a chance to escape Capture and examine the contents of main memory on running systems Walk through the unraveling of an intrusion, one step at a time The book"s companion Web site contains complete source and binary code for open source software discussed in the book, plus additional computer forensics case studies and resource links.

Forensic Discovery

When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world.Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more.Practical Unix & Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats.

Practical UNIX and Internet Security

Network Fundamentals, CCNA Exploration Companion Guide is the official supplemental textbook for the Network Fundamentals course in the Cisco® Networking Academy® CCNA® Exploration curriculum version 4. The course, the first of four in the new curriculum, is based on a top-down approach to networking. The Companion Guide, written and edited by Networking Academy instructors, is designed as a portable desk reference to use anytime, anywhere. The book's features reinforce the material in the course to help you focus on important concepts and organize your study time for exams. New and improved features help you study and succeed in this course: Chapter objectives–Review core concepts by answering the focus questions listed at the beginning of each chapter. Key terms–Refer to the updated lists of networking vocabulary introduced and highlighted in context in each chapter. Glossary–Consult the comprehensive glossary with more than 250 terms. Check Your Understanding questions and answer key–Evaluate your readiness with the updated end-of-chapter questions that match the style of questions you see on the online course quizzes. The answer key explains each answer. Challenge questions and activities–Strive to ace more challenging review questions and activities designed to prepare you for the complex styles of questions you might see on the CCNA exam. The answer key explains each answer. How To–Look for this icon to study the steps you need to learn to perform certain tasks. Packet Tracer Activities– Explore networking concepts in activities interspersed throughout some chapters using Packet Tracer v4.1 developed by Cisco. The files for these activities are on the accompanying CD-ROM. Also available for the Network Fundamentals Course Network Fundamentals, CCNA Exploration Labs and Study Guide ISBN-10: 1-58713-203-6 ISBN-13: 978-1-58713-203-2 Companion CD-ROM **See instructions within the ebook on how to get access to the files from the CD-ROM that accompanies this print book.** The CD-ROM provides many useful tools and information to support your education: Packet Tracer Activity exercise files v4.1 VLSM Subnetting Chart Structured Cabling Exploration Supplement Taking Notes: a .txt file of the chapter objectives A Guide to Using a Networker's Journal booklet IT Career Information Tips on Lifelong Learning in Networking This book is part of the Cisco Networking Academy Series from Cisco Press®. The products in this series support and complement the Cisco Networking Academy online curriculum.

Network Fundamentals, CCNA Exploration Companion Guide

Python Forensics provides many never-before-published proven forensic modules, libraries, and solutions that can be used right out of the box. In addition, detailed instruction and documentation provided with the code samples will allow even novice Python programmers to add their own unique twists or use the models presented to build new solutions. Rapid development of new cybercrime investigation tools is an essential ingredient in virtually every case and environment. Whether you are performing post-mortem investigation, executing live triage, extracting evidence from mobile devices or cloud services, or you are collecting and processing evidence from a network, Python forensic implementations can fill in the gaps. Drawing upon years of practical experience and using numerous examples and illustrative code samples, author Chet Hosmer discusses how to: Develop new forensic solutions independent of large vendor software release schedules Participate in an open-source workbench that facilitates direct involvement in the design and implementation of new methods that augment or replace existing tools Advance your career by creating new solutions along with the construction of cutting-edge automation solutions to solve old problems Provides hands-on tools, code samples, and detailed instruction and documentation that can be put to use immediately Discusses how to create a Python forensics workbench Covers effective forensic searching and indexing using Python Shows how to use Python to examine mobile device operating systems: iOS, Android, and Windows 8 Presents complete coverage of how to use Python scripts for network investigation

Python Forensics

A comprehensive guide to the threats facing Apple computers and the foundational knowledge needed to become a proficient Mac malware analyst. Defenders must fully understand how malicious software works if they hope to stay ahead of the increasingly sophisticated threats facing Apple products today. The Art of Mac Malware: The Guide to Analyzing Malicious Software is a comprehensive handbook to cracking open these malicious programs and seeing what's inside. Discover the secrets of nation state backdoors, destructive ransomware, and subversive cryptocurrency miners as you uncover their infection methods, persistence strategies, and insidious capabilities. Then work with and extend foundational reverse-engineering tools to extract and decrypt embedded strings, unpack protected Mach-O malware, and even reconstruct binary code. Next, using a debugger, you'll execute the malware, instruction by instruction, to discover exactly how it operates. In the book's final section, you'll put these lessons into practice by analyzing a complex Mac malware specimen on your own. You'll learn

to: Recognize common infections vectors, persistence mechanisms, and payloads leveraged by Mac malware Triage unknown samples in order to quickly classify them as benign or malicious Work with static analysis tools, including disassemblers, in order to study malicious scripts and compiled binaries Leverage dynamical analysis tools, such as monitoring tools and debuggers, to gain further insight into sophisticated threats Quickly identify and bypass anti-analysis techniques aimed at thwarting your analysis attempts A former NSA hacker and current leader in the field of macOS threat analysis, Patrick Wardle uses real-world examples pulled from his original research. The Art of Mac Malware: The Guide to Analyzing Malicious Software is the definitive resource to battling these ever more prevalent and insidious Apple-focused threats.

The Art of Mac Malware

bull; Real-world tools needed to prevent, detect, and handle malicious code attacks. bull; Computer infection from viruses, worms, Trojan Horses etc., collectively known as malware is a growing cost problem for businesses. bull; Discover how attackers install malware and how you can peer through their schemes to keep systems safe. bull; Bonus malware code analysis laboratory.

Malware

Geneen Roth, author of the #1 New York Times bestseller Women Food and God, explains how to take the journey to find one’s own best self in this “beautiful, funny, deeply relevant” (Glennon Doyle) collection of personal reflections. With an introduction by Anne Lamott, This Messy Magnificent Life is a personal and exhilarating read on freeing ourselves from daily anxiety, lack, and discontent. It’s a deep dive into what lies behind our self-criticism, whether it is about the size of our thighs, the expression of our thoughts, or the shape of our ambitions. And it’s about stopping the search to fix ourselves by realizing that on the other side of the “Me Project” is spaciousness, peace, and the capacity to reclaim one’s power and joy. This Messy Magnificent Life explores the personal beliefs, hidden traumas, and social pressures that shape not just women’s feelings about their bodies but also their confidence, choices, and relationships. After years of teaching retreats and workshops on weight, money, and other obsessions, Roth realized that there was a connection that held her students captive in their unhappiness. With laugh-out-loud humor, compassion, and dead-on insight she reveals the paradoxes in our beliefs and shows how to move beyond our past to build lives that reflect our singularity and inherent power. This Messy Magnificent Life is a brilliant, bravura meditation on who we take ourselves to be, what enough means in our gotta-get-more culture, and being at home in our minds and bodies.

This Messy Magnificent Life

Writers Forensics A Dp Guide For Lyle

CWA London Chapter – In Conversation with DP Lyle, and Simon Bewick & Vic Watson - CWA London Chapter – In Conversation with DP Lyle, and Simon Bewick & Vic Watson by The Crime Writers' Association 44 views 3 years ago 52 minutes - The CWA's London chapter hosts an evening of conversation with **DP Lyle**,, **author**, of 'Deep Six', 'Skin in the Game', and the ...
How Do You Corral Your Own Writing Time
Typical Writing Session
The Hair Follicles
How Did You Get Interested in Poisons
The One Punch Knockout
Instant Rigor Mortis
How To Commit the Perfect Murder
Christmas Short Story Competition
Forensics For Dummies: 2nd Edition by D.P. Lyle, MD · Audiobook preview - Forensics For Dummies: 2nd Edition by D.P. Lyle, MD · Audiobook preview by Google Play Books 16 views 2 months ago 1 hour, 49 minutes - Forensics, For Dummies: 2nd Edition Authored by D.P. **Lyle**,, MD Narrated by Chris Sorensen #dplylemd ...
Peter James | DP Lyle | Authors Studio - Meet The Masters - Peter James | DP Lyle | Authors Studio - Meet The Masters by Peter James TV 247 views 5 years ago 5 minutes, 47 seconds - Multiple award winning **DP Lyle**, is a doctor, a mystery **writer**, and also a non fiction **writer**, - with his famous book '**Forensics**, For ...

Give one writing tip
Where & when do you write?
books that inspired you?
Do you have any ritual before you start writing?
How do you plan a book?
BookTrib | D.P. Lyle On How He Writes | Forensics | Murder Mayhem | Stress Fracture - BookTrib | D.P. Lyle On How He Writes | Forensics | Murder Mayhem | Stress Fracture by BookTrib 62 views 8 years ago 3 minutes, 5 seconds - World-renowned **Forensic**, Science **author**, D.P. **Lyle**, chats with BookTrib about how he begins the **writing**, process and how his ...
Author Interview: Alison May on Forensic Linguistics - Author Interview: Alison May on Forensic Linguistics by Taylor & Francis Books 2,210 views 3 years ago 8 minutes, 1 second - What is **forensic**, linguistics? What impact does it have in the legal system? Is it possible to identify an individual **author**, through ...
Introduction
What does forensic linguistics cover
Why is forensic linguistics important
Most interesting forensic linguistics case
Future trends in forensic linguistics
How To Write A Literature Review From Start To Finish (Advanced Tactics For PhDs And Researchers) - How To Write A Literature Review From Start To Finish (Advanced Tactics For PhDs And Researchers) by Academic English Now 71,750 views 1 year ago 1 hour, 13 minutes - 00:00 - Intro 04:11 - Avoid waffling 10:50 - Learn more, book in a free call 34:57 - Focusing on one study in more detail 43:32 ...
Intro
Avoid waffling
Learn more, book in a free call
Focusing on one study in more detail
Pattern variation
Linking your ideas together
How To Write An Exceptional Literature Review With AI [NEXT LEVEL Tactics] - How To Write An Exceptional Literature Review With AI [NEXT LEVEL Tactics] by Andy Stapleton 183,957 views 3 months ago 14 minutes, 22 seconds - In this video I share with you to write a literature review with AI using next level tactics some incredible tools. ½ ½ Sign up for my ...
create structure
find papers
import
explore your documents
wrapping up
WRITING CHAPTER 2: LITERATURE REVIEW - WRITING CHAPTER 2: LITERATURE REVIEW by Platform for Research & Development 9,291 views Streamed 1 year ago 1 hour, 29 minutes - This session covers contents to be included in a PhD/DBA Thesis or Dissertations.
Literature Review
Theoretical Framework
What Is a Literature Review
Why We Need a Literature Review
Where To Start
Dependent Variable
Independent Variables
Chronological
Underpinning Theory
Justification
Conclusion
Question and Answers
Why Carrying Out the Literature Review
Is It Necessary to To Incorporate the Underpinning Theories
How To Synthesize the Research Theories
Journal Selection
Conceptual Framework
Building Blocks of Theories

Conceptual Theory
Debate
Why Choose Your Country
How To Identify a Good Journal
How Can You Write Research Problem
The Dependent Differentiation between Qualitative Quantitative Literature Review
Avoid Plagiarism
Seven Golden Rules To Avoid Plagiarism
How To Avoid Plagiarism
How Many Papers Is Required for a Review Article for Publication
Find A Research Gap In ONE Day (Step-by-step Tutorial) - Find A Research Gap In ONE Day (Step-by-step Tutorial) by Academic English Now 35,711 views 1 year ago 8 minutes, 48 seconds - 00:00 - Intro 01:33 - #1 Look up the most recent papers 04:09 - #2 Jump to the conclusion or the end of the discussion 05:58 - #3 ...
Intro
1 Look up the most recent papers
2 Jump to the conclusion or the end of the discussion
3 Look at the suggestions for future research
Book in a free call
Literature Review Writing 2021: How to write a literature review FAST with example - Literature Review Writing 2021: How to write a literature review FAST with example by Dr B - Naija Dentist 102,925 views 3 years ago 32 minutes - In this video you will learn how to write a Literature review. **Writing**, a literature review can be quite tedious. However, this video is ...
Introduction
Why literature review
How to search for literatures
What to write
Example 1
Example 2
Outro
The Quickest Way To Write A First Class Literature Review | IN JUST 5 EASY STEPS - The Quickest Way To Write A First Class Literature Review | IN JUST 5 EASY STEPS by Dr Amina Yonis 90,645 views 1 year ago 12 minutes, 31 seconds - Chapter Timestamps 00:00 Introduction 00:50 The search terms 03:20 A reading summary 04:15 Automatic editing 07:40 ...
Introduction
The search terms
A reading summary
Automatic editing
Structure first
Linker sentences
Literature Review - Step by Step Guide For Graduate Students | Prof. David Stuckler - Literature Review - Step by Step Guide For Graduate Students | Prof. David Stuckler by David Stuckler 143,511 views 2 years ago 19 minutes - Are you stuck **writing**, your literature review? If so, you must watch this video. This video will break down the whole process into ...
Intro
What is literature review?
Finding structure
“Strip method”
Developing the conceptual framework
The snowball method
The PEER system
PEER system in practice
Writing your conclusion and intro
2.3 Let's Write: First Lines and Literature Review Of Research Thesis - 2.3 Let's Write: First Lines and Literature Review Of Research Thesis by MeanThat 490,921 views 8 years ago 20 minutes - YouTube is a bit limiting when it comes to online lecturing. If you would like to see our full online courses with assignments, ...
Introduction
Research Idea

Structure
Google Drive
Reference Generator
Intext Reference
How to write a literature review fast I write a lit review fast! - How to write a literature review fast I write a lit review fast! by Dr Dee 562,294 views 3 years ago 5 minutes, 38 seconds - Covers everything you need to know about how to write a literature review fast. It provides a template to get you started quickly to ...
Intro
What is a literature review
What should be our first step
Step 1 Search
Step 2 Evaluate
Step 3 File Sources
Step 4 Create Annotated Bibliography
Step 5 Organize
Literature review structure for a PhD thesis (3 easy steps) - Literature review structure for a PhD thesis (3 easy steps) by Academic English Now 20,941 views 3 years ago 5 minutes, 33 seconds - Book a free 1-1 consultation: https://academicenglishnow.com/schedule?utm_source=YouTube&utm_content=15-07-2020 If you ...
Write The Literature Review In Just 2 Hours (LIVE Writing Session) - Write The Literature Review In Just 2 Hours (LIVE Writing Session) by Academic English Now 13,937 views 1 year ago 2 hours, 3 minutes - Schedule a free 1-1 strategy session with me to see how I can help you achieve your research goals: ...
10 Ways To Use ChatGPT To Write Research Papers (ETHICALLY) In 2023 - 10 Ways To Use ChatGPT To Write Research Papers (ETHICALLY) In 2023 by Academic English Now 495,218 views 9 months ago 25 minutes - 00:00 - Intro 03:53 - #1 Research paper titles using ChatGPT 07:04 - #2 **Writing**, an abstract using ChatGPT 08:51 - #3 **Writing**, a ...
Intro
1 Research paper titles using ChatGPT
2 Writing an abstract using ChatGPT
3 Writing a research gap using ChatGPT
4 Writing a research question using ChatGPT
5 Making a research question more specific
6 Writing a literature review using ChatGPT
7 Structure of a literature review using ChatGPT
8 Writing an introduction using ChatGPT
9 Writing an introduction on a topic that hasn't been published yet using ChatGPT
10 Writing an introduction from the abstract using ChatGPT
Write The Literature Review: 4 EASY Steps (Implement TODAY) - Write The Literature Review: 4 EASY Steps (Implement TODAY) by Academic English Now 27,244 views 1 year ago 38 minutes - 00:00 - Intro 00:30 - The breakdown 02:36 - Finding the text 07:35 - Inclusion and exclusion criteria 13:05 - Reading your papers ...
Intro
The breakdown
Finding the text
Inclusion and exclusion criteria
Reading your papers
Structuring and organizing
Writing the literature review
Book in a free call
How To Write A Literature Review From Start To Finish (Full Tutorial) - How To Write A Literature Review From Start To Finish (Full Tutorial) by Academic English Now 26,878 views 1 year ago 12 minutes, 9 seconds - 00:00 - Intro 01:10 - Identify the main topics 03:39 - Identify the subtopics 04:33 - Clarify the destination 06:16 - Be more critical ...
Intro
Identify the main topics
Identify the subtopics
Clarify the destination

Be more critical
Structure the literature review
Show the logic to the reader
Book in a call At Academic English Now we support PhD students and researchers in publishing research papers in Q1 Scopus-Indexed journals. We are apssionate about helping researchers and PhD students express their research ideas with greater confidence. We have worked with 400+ researchers and PhD students. Our clients have published in Q1 Scopus-indexed journals, including such renown journals as Nature Ecology & Evolution.
The format and language of a literature review - The format and language of a literature review by cecile badenhorst 4,100 views 3 years ago 17 minutes - If you are a master's or doctoral **writer writing**, a literature review for coursework, a thesis or a paper for publication, this video is for ...
state the aim of the review
draw conclusions based on your analysis of the literature
organize the literature chronologically according to publication
develop an entry point for your argument through the literature
identify a key research question
provide short short summaries of the research studies of your readings
outline a plan for writing the literature review
focus on transition words and phrases
Background Research - Background Research by Zara Altair 23 views Streamed 4 years ago 17 minutes - Introduction to research for a mystery novel. Sources and procedures. Links to research: * What's What, by David Fisher and ...
Intro
Background Research
Word of Mouth
Online Research
Real Estate
Crime Writing
Research Guidelines
Conclusion
IB ENGLISH A: Paper 1 Checklist - WATCH 5 MINUTES BEFORE EXAMS! - IB ENGLISH A: Paper 1 Checklist - WATCH 5 MINUTES BEFORE EXAMS! by IB English Guys 70,268 views 10 months ago 4 minutes, 32 seconds - This video provides a checklist to ace Paper 1. Check us out at https://ibenglishguys.com/ Free document: ...
4 TIPS for Writing a Literature Review's Intro, Body & Conclusion | Scribbr ⇐“4 TIPS for Writing a Literature Review's Intro, Body & Conclusion | Scribbr ⇐by Scribbr 751,924 views 3 years ago 4 minutes, 30 seconds - Just like any other academic text, your literature review should have an introduction, a main body, and a conclusion. In this video ...
Intro
General structure
Introduction
Body
4 Tips for main body
1. Summarize & synthesize
2. Analyze and interpret
3. Critically evaluate
4. Use well-structured paragraphs
Conclusion
Before submitting
Writing the Literature Review - Writing the Literature Review by Academic Skills, The University of Melbourne 368,087 views 6 years ago 10 minutes, 24 seconds - This video looks at literature review - how to evaluate reading, critical questions of texts, language of literature review and some ...
Introduction
Defining a Literature Review
Evaluating Sources
Writing
Critique
Checklist
LITERATURE REVIEW Tutorial: Writing the Literature Review Real Example - LITERATURE REVIEW

Tutorial: Writing the Literature Review Real Example by Smart Student 147,536 views 2 years ago 39 minutes - ---- SMART STUDENT FACEBOOK GROUP http://www.facebook.com/groups/communitysmartstudent/ SAY HI ON ...
Introduction
What a literature review is
How to organize your sources
How to structure your paper
Write the literature review tutorial
APL110 - Forensic Linguistics - An Overview - APL110 - Forensic Linguistics - An Overview by The Virtual Linguistics Campus 32,239 views 9 years ago 12 minutes - In this overview of **Forensic**, linguistics, Prof. Handke discusses the central goals of this new and growing disipline, as well as the ...
Introduction
Central Principles
Technical Issues
Forensic Texts
Linguistic Features
Grammar and Vocabulary
Examples
Search filters
Keyboard shortcuts
Playback
General
Subtitles and closed captions
Spherical videos

Malware Forensics Field For Linux Systems Digital Forensics Field S

TryHackMe! Linux Server Forensics Walkthrough - TryHackMe! Linux Server Forensics Walkthrough by Jason Turley 1,566 views 1 year ago 47 minutes - In this video, we will investigate three compromised **Linux**, servers and learn about attacker techniques! Like, comment and ...
Top 10 forensic artefacts and data sources on Linux - Top 10 forensic artefacts and data sources on Linux by Mossé Cyber Security Institute 1,456 views 1 year ago 4 minutes, 54 seconds - Linux forensics, is the process of identifying, extracting, and analyzing data from a **Linux system**, for the purpose of determining the ...
Linux Forensics Investigation | TryHackMe Linux Forensics - Linux Forensics Investigation | TryHackMe Linux Forensics by Motasem Hamdan 6,865 views 1 year ago 28 minutes - In this video walk-through, we covered auditing **Linux**, workstations for **forensic**, information as part of TryHackMe **Linux Forensics**,.
Default Shell
Running Processes
Log Files
Log File
Task 7
Analyzing a malware sample with Memory Forensics - Analyzing a malware sample with Memory Forensics by Mossé Cyber Security Institute 2,078 views 1 year ago 13 minutes, 57 seconds - In this video we will demonstrate a piece of **malware**, being analyzed with memory **forensics**,. These techniques can be applied to ...
Lab Tour: Cyber Forensics Lab at NIWC Atlantic - Lab Tour: Cyber Forensics Lab at NIWC Atlantic by Naval Information Warfare Systems Command - NAVWAR 3,522 views 1 year ago 2 minutes, 10 seconds - The **Cyber Forensics**, Lab is comprised of two main specialties. Data recovery and **forensics**, examination. These capabilities ...
Memory Forensics with Volatility | HackerSploit Blue Team Series - Memory Forensics with Volatility | HackerSploit Blue Team Series by Akamai Developer 8,742 views 1 year ago 34 minutes - Volatility is an open source memory **forensics**, framework for incident response and **malware**, analysis. In this video, @HackerSploit ...
Introduction
What We Will Be Covering
Pre Requisites

Introduction to Volatility
Learning Resources
Practical Demo
What is Volatility?
Using MemLabs to Simulate a Crash/Compromise
Install Volatility
Transfer MemLabs Files to this System
Install and Extract the MemLabs File
Open the Dump in Volatility
Perform KDBG Scan
Extracting Information
Identify Hidden Processes
Investigate What a Process Was Doing
What Commands Were Being Executed?
Scan and Extract a File
Obtain Hashes with Volatility & CyberChef
Exploring Additional Modules
Conclusion
DFIR 101: Digital Forensics Essentials | Kathryn Hedley - DFIR 101: Digital Forensics Essentials | Kathryn Hedley by SANS Digital Forensics and Incident Response 30,472 views 2 years ago 1 hour, 16 minutes - Whether you're new to the **field**, of **digital forensics**,, are working in an entirely different role, or are just getting into cybersecurity, ...
Intro
Overview
Digital Evidence
Data and Metadata
Data
Metadata
File System Metadata
Word Metadata
The BTK Killer
Data Interpretation
Binary
One byte
hexadecimal
sectors and clusters
allocated and unallocated
slack space
ram slack
unused space
deleted space
file slack
file systems
Where do we find digital evidence
Digital investigation
Types of investigations
Instant response and threat hunting
Documented media exploitation
Other military action
Auditing
Internal Investigations
Legal Cases
Summary
Digital Forensics
What now
Whats the purpose
Introduction to Digital Forensics and Incident Response | TryHackMe DFIR - Introduction to Digital Forensics and Incident Response | TryHackMe DFIR by Motasem Hamdan 4,846 views 1 year ago 22 minutes - In this video walk-through, we covered basic and essential concepts and tools in **Digital**

Forensics, and Incident Response.
Digital Forensics Full Course With Practicals - First On YouTube [Hindi] - Digital Forensics Full Course With Practicals - First On YouTube [Hindi] by Defronix Academy 18,997 views 6 months ago 4 hours, 15 minutes - We bring you the most demanded & talk of the town topic in this video. Presenting you **Digital Forensics**, Full Course With ...
Module 1: Introduction & Fundamentals of Digital Forensics
Module 2: Forensics Data Acquisition
Module 3: Forensic Analysis of Different Files
Module 4: Forensics File Carving & Recovery
Module 5: Autopsy Operations
Module 6: Memory Forensics
Module 7: Network Forensics with Wireshark
Module 8: Reporting & Documentation
Wrapping Up
Best digital forensics | computer forensics| cyber forensic free tools - Best digital forensics | computer forensics| cyber forensic free tools by Information Security Newspaper 116,258 views 3 years ago 25 minutes - THIS VIDEO IS FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY. WE DO NOT PROMOTE, ENCOURAGE, ...
This is the operating system Edward Snowden recommends - This is the operating system Edward Snowden recommends by censiCLICK 2,014,994 views 3 years ago 4 minutes, 45 seconds - Support the channel on Patreon: https://www.patreon.com/censiclick Famous NSA whistleblower Edward Snowden for many is a ...
Investigating Malware Using Memory Forensics - A Practical Approach - Investigating Malware Using Memory Forensics - A Practical Approach by Black Hat 74,695 views 4 years ago 1 hour, 3 minutes - This presentation mainly focuses on the practical concept of memory **forensics**, and shows how to use memory **forensics**, to detect, ...
Investigating Malware Using Memory Forensics - A Practical Approach
Monnappa KA • Info Security Investigator - Cisco CSIRT • Author of the Book: Learning Malware Analysis • Member of Black Hat Review Board • Co-founder Cysinfo Security Community • Creator of Limon Sandbox • Winner of Volatility Plugin Contest 2016
Memory Acquisition - Dumping the memory of a target machine to disk
Memory Analysis of Infected System (KeyBase Malware)
Memory Analysis of Infected System (Darkcomet RAT)
Investigating Hollow Process Injection
Investigating Rootkits
Memory Analysis of ZeroAccess Rootkit
Example - Memory Analysis of Necurs Rootkit
Detecting & Hunting Ransomware Operator Tools: It Is Easier Than You Think! - Detecting & Hunting Ransomware Operator Tools: It Is Easier Than You Think! by SANS Digital Forensics and Incident Response 18,279 views 11 months ago 1 hour, 21 minutes - Ryan Chapman, SANS Instructor and author of SANS FOR528: **Ransomware**, for Incident Responders, provides an overview of ...
Digital Forensics Course | Digital Forensics for Beginners | NetCom Learning - Digital Forensics Course | Digital Forensics for Beginners | NetCom Learning by NetCom Learning 26,607 views Streamed 2 years ago 2 hours, 25 minutes - In this video on **Digital Forensics**, Course, you will be learning about what is **Digital Forensic**,, Fundamentals of Computer ...
Digital Forensics Course
Understanding Computer Forensic
Types of Cyber crimes
Impact of cyber crimes at organisational level
Introduction to digital evidence
Roles and responsibilities of Forensics investigator
Computer forensics and legal compliance
Importance of the Forensic investigator
Setting up a computer Forensic lab
Gathering and organising information
Writing the investigation report
What is booting process?
Data acquisition methodology
Challenges in web applications forensics

Indicators of a web attack
Web application threats
Introduction to an email system
Windows Forensics P2 | The File System | TryHackMe Cyber Defense - Windows Forensics P2 | The File System | TryHackMe Cyber Defense by Motasem Hamdan 642 views 2 months ago 34 minutes - In this video walkthrough, we covered the second part of Windows **OS forensics**, where we demonstrated gathering artifacts from ...
How to set up a digital forensics lab | Cyber Work Hacks - How to set up a digital forensics lab | Cyber Work Hacks by Infosec 6,388 views 1 year ago 8 minutes, 55 seconds - Infosec Skills author and Paraben founder and CEO Amber Schroader talks about how to quickly and inexpensively set up your ...
Creating your digital forensics lab
Benefits of your own digital forensics lab
Space needed for digital forensics lab
Essential hardware needed for a forensics lab
Important forensic lab upgrades
Running your forensics lab
Forensic lab projects
Getting into forensic labs
Outro
Introduction to Windows Forensics - Introduction to Windows Forensics by 13Cubed 160,029 views 6 years ago 1 hour, 4 minutes - An introduction to basic Windows **forensics**,, covering topics including UserAssist, ShellBags, USB devices, network adapter ...
Introduction
The Windows Registry
Into User Data
Shellbags
User Class BAT
USB Devices
USB Store
Software
Mounted Devices
Serial Number
Volume Good
USB Device
Miscellaneous Registry Keys
Network Location Awareness
Linked Files
Prefecture Superfetch
Master Wireshark: Your Ultimate Guide to Hunting Cyber Villains! ≈¸Master Wireshark: Your Ultimate Guide to Hunting Cyber Villains! ≈by LearnLadder 1,100 views 4 days ago 2 hours, 34 minutes - Dive deep into the world of cybersecurity and unlock the secrets of network analysis with "Master Wireshark: Your Ultimate Guide ...
Introduction
Packet Level Analysis for Incident Response
Host and Network Discovery Techniques
Importance of Detecting Network Scans
Lab 1: Detecting Network Discovery Scans
Lab 2: Detecting Port Scans Techniques
Understanding Layer 3 Scanning
TCP SYN Scan Explained
Introduction to Lab 3
Lab 3: Trace File Analysis with pcapng
Lab 3: Trace File Analysis - Questions and Answers
OS Fingerprinting Techniques
Lab 4: Practicing OS Fingerprinting
HTTP Path Enumeration Methods
Enumerating Web Servers Strategies
Identifying Suspect Traffic Patterns

Detecting Unusual Port Numbers
Lab 6: Unusual TCP SYN Scans Detection
Lab 7: Advanced Detection Techniques
Lab 8: Specialized Packet Analysis
Traffic Pattern 5: Unencrypted Web Traffic Analysis
Traffic Pattern 6: Analyzing Outdated TLS and Bad User Agents
Lab 9: Unencrypted HTTP File Transfer Detection
Key Traffic Patterns to Monitor
Lab 10: Analyzing FTP Server Brute Force Attack
Module 11 Introduction
Understanding Malware Basics
Malware Analysis Techniques with Wireshark
Filtering Common Traffic in Analysis
Examining Traffic to Port 8082
What's Next in Packet Analysis
Key Learnings from Packet Analysis
Reverse Shell Traffic Analysis
Lab 12: Reverse Shell Detection
Understanding Botnet Traffic
Analyzing Botnet Traffic Techniques
Data Exfiltration Concepts
FTP Data Exfiltration Analysis
FORENSIC ANALYSIS USING AUTOPSY Linux and Windows - FORENSIC ANALYSIS USING AUTOPSY Linux and Windows by Computing for All 14,426 views 2 years ago 31 minutes - By: Mr. Sridhar Chandramohan Iyer.
Extracting Information from RAM? Memory Dump analysis with VOLATILITY (Digital Forensics- THM) - Extracting Information from RAM? Memory Dump analysis with VOLATILITY (Digital Forensics- THM) by Hox Framework 5,155 views 2 years ago 12 minutes, 33 seconds - - Also thanks for all the new subs! If anyone is interested in getting into the community you can also join our discord (link on the ...
Best Forensic and Pentesting Linux Distros in 2022 - Best Forensic and Pentesting Linux Distros in 2022 by Knowledge Power 2,429 views 1 year ago 4 minutes, 9 seconds - cybersecurity #pentesting #**linux**, Best **Forensic**, and Pentesting **Linux**, Distros in 2022.
Is your PC hacked? RAM Forensics with Volatility - Is your PC hacked? RAM Forensics with Volatility by The PC Security Channel 883,730 views 1 year ago 14 minutes, 29 seconds - In this video we explore advanced memory **forensics**, in Volatility with a RAM dump of a hacked **system**,. Workshop: ...
Autopsy - Forensic Acquisition Tool | Digital Forensics Investigation | Autopsy Tutorial - Autopsy - Forensic Acquisition Tool | Digital Forensics Investigation | Autopsy Tutorial by Free Education Academy - FreeEduHub 64,781 views 2 years ago 23 minutes - In this video, we will use Autopsy as a **forensic**, Acquisition tool. Its the best tool available for **digital forensics**,. I will explain all ...
Cybersecurity Expert Demonstrates How Hackers Easily Gain Access To Sensitive Information - Cybersecurity Expert Demonstrates How Hackers Easily Gain Access To Sensitive Information by Dr. Phil 3,194,532 views 4 years ago 3 minutes, 27 seconds - Cybersecurity expert Kevin Mitnick demonstrates how today's “crackers”, “gearheads” and “cyberpunks” illegally access sensitive ...
Introduction to Digital Forensics - Learn the Basics - Introduction to Digital Forensics - Learn the Basics by Prabh Nair 10,311 views 1 year ago 36 minutes - In this video i have covered : 1)What is #cybercrime 2) What is **Digital Forensics**, 3) Tools used in **Digital forensics**, Investigation 4) ...
Chain of Custody
Creating an investigation strategy
Tools used in Digital Investigation
The Linux Forensics tools you need to learn and master - The Linux Forensics tools you need to learn and master by Mossé Cyber Security Institute 948 views 1 year ago 4 minutes, 11 seconds - Linux forensics, tools are used to help investigate cases of data breaches and **system**, intrusions. These tools can be used to ...
My life as Cyber Forensic Investigator and what Certifications you should - My life as Cyber Forensic Investigator and what Certifications you should by UnixGuy | Cyber Security 60,135 views 1 year ago 12 minutes, 37 seconds - I'm sharing with you what my life looked like as a **Cyber Forensic**, Investigator, the crimes that I investigated, the good and the bad ...

Intro
cctv footage
timeline
Certifications
Digital Forensics: How Malware Can Hide In Plain Sight - Digital Forensics: How Malware Can Hide In Plain Sight by Lawrence Systems 10,850 views 3 years ago 14 minutes, 55 seconds - Connecting With Us ---------- + Hire Us For A Project: https://lawrencesystems.com/hire-us/ + Tom ...
Linux Forensics Tutorial || Linux file system forensics - Linux Forensics Tutorial || Linux file system forensics by CS Lesson 10,829 views 3 years ago 1 hour, 50 minutes - This video presents #**Linux**, #filesystem #**forensics**, ℞Permission ℞This video was published by " linuxfestnorthwest" and ...
Introduction
The Scenario
The Disk Image
Converting from VMDK to Raw Format
Notes About Linux Filesystems
Filesystem Timestamps
Demo
Search filters
Keyboard shortcuts
Playback
General
Subtitles and closed captions
Spherical videos