Understanding Network Forensics Analysis In An Operational

UNDERSTANDING NETWORK FORENSICS ANALYSIS IN AN OPERATIONAL DOWNLOAD PDF

Invite to our collection, where you can easily download Understanding Network Forensics Analysis In An Operational to boost your discovering and research study experience. Our vast collection of PDF documents can supply important educational sources that accommodate different topics and interests. We comprehend the significance of accessing info promptly and easily, so we make every effort to make the procedure of **downloading and install Understanding Network Forensics Analysis In An Operational PDF** from our platform simple and hassle-free. With simply a few clicks, you can unlock a globe of expertise from our library without any obstacles. Join us in exploring our extensive collection and begin your PDF downloads today!

EXPLORING OUR EXTENSIVE COLLECTION INCLUDING UNDERSTANDING NETWORK FORENSICS ANALYSIS IN AN OPERATIONAL

Learning Network Forensics Walter de Gruyter GmbH & Co KG

Network ForensicsJohn Wiley & Sons

Digital Evidence and Computer Crime Syngress

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks.

There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today’s organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders’ abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

Unified Communications Forensics Network Forensics

Electronic discovery refers to a process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case. Computer forensics is the application of computer investigation and analysis techniques to perform an investigation to find out exactly what happened on a computer and who was responsible. IDC estimates that the U.S. market for computer forensics will be grow from $252 million in 2004 to

$630 million by 2009. Business is strong outside the United States, as well. By 2011, the estimated international market will be $1.8 billion dollars. The Techno Forensics Conference has increased in size by almost 50% in its second year; another example of the rapid growth in the market. This book is the first to combine cybercrime and digital forensic topics to provides law enforcement and IT security professionals with the information needed to manage a digital investigation. Everything needed for analyzing forensic data and recovering digital evidence can be found in one place, including instructions for building a digital forensics lab. * Digital investigation and forensics is a growing industry * Corporate I.T. departments investigating corporate espionage and criminal activities are learning as they go and need a comprehensive guide to e-discovery * Appeals to law enforcement agencies with limited budgets

Investigate network attacks and find evidence using common network forensic tools IGI Global

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book's 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students' understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book.

Cybersecurity & Digital Forensics Syngress

An up-to-date, comprehensive, practical, guide to network forensics for information security professionals at all levels of experience * *Presents a proven, start-to-finish methodology for managing any network forensics investigation. *Enables professionals to uncover powerful forensic evidence from routers, firewalls, IDS, web proxies, and many other network devices. *Based on the world's first comprehensive Network Forensics training course, offered by the SANS Institute - a course that now sells out months in advance. Network forensics is transforming the way investigators examine computer crime: they have discovered that the network holds far more evidence than could ever be retrieved from a local hard drive. Network forensic skills are in especially short supply, and professionals are flocking to the scarce resources available for mastering these skills. This is a

comprehensive, practical, and up to- date book on the subject. Building on their pioneering SANS Institute course, top network forensics experts Jonathan Ham and Sherri Davidoff take readers through an exciting, entertaining, and technically rigorous journey through the skills and principles of successful network investigation. One step at a time, they demonstrate how to recover usable forensic evidence from firewalls, web proxies, IDS, routers, wireless access points, and even raw packet captures. Coverage includes: * *Understanding the unique challenges associated with network investigation. *The state-of-the-art OSCAR Network Forensics Investigative Methodology. *Acquiring evidence passively, actively, and interactively. *Aggregating, correlating, and analyzing event logs. *Investigating compromised encryption and SSL interception Every section contains a real-world case study, and the book culminates with a 'Capstone' case study walking through an entire investigation from start to finish, and challenging readers to solve the crime themselves.

Information and Communication Technologies Jones & Bartlett Learning

Cisco IOS (the software that runs the vast majority of Cisco routers and all Cisco network switches) is the dominant routing platform on the Internet and corporate networks. This widespread distribution, as well as its architectural deficiencies, makes it a valuable target for hackers looking to attack a corporate or private network infrastructure. Compromised devices can disrupt stability, introduce malicious modification, and endanger all communication on the network. For security of the network and investigation of attacks, in-depth analysis and diagnostics are critical, but no book currently covers forensic analysis of Cisco network devices in any detail. Cisco Router and Switch Forensics is the first book devoted to criminal attacks, incident response, data collection, and legal testimony on the market leader in network devices, including routers, switches, and wireless access points. Why is this focus on network devices necessary? Because criminals are targeting networks, and network devices require a fundamentally different approach than the process taken with traditional forensics. By hacking a router, an attacker can bypass a network's firewalls, issue a denial of service (DoS) attack to disable the network, monitor and record all outgoing and incoming traffic, or redirect that communication anywhere they like. But capturing this criminal activity cannot be accomplished with the tools and techniques of traditional forensics. While forensic analysis of computers or other traditional media typically involves immediate shut-down of the target machine, creation of a duplicate, and analysis of static data, this process rarely recovers live system data. So, when an investigation focuses on live network activity, this traditional approach obviously fails. Investigators must recover data as it is transferred via the router or switch, because it is destroyed when the network device is powered down. In this case, following the traditional approach outlined in books on general computer forensics techniques is not only insufficient, but also essentially harmful to an investigation. Jargon buster: A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). A router is a more sophisticated network device that joins multiple wired or wireless networks together. The only book

devoted to forensic analysis of routers and switches, focusing on the operating system that runs the vast majority of network devices in the enterprise and on the Internet Outlines the fundamental differences between router forensics and traditional forensics, a critical distinction for responders in an investigation targeting network activity Details where network forensics fits within the entire process of an investigation, end to end, from incident response and data collection to preparing a report and legal testimony

At our system, we take satisfaction in our substantial collection of PDF data consisting of Understanding Network Forensics Analysis In An Operational that accommodate various interests and fields of research study. Whether you are aiming to broaden your understanding or performing research, we have a wide range of PDFs that make certain to satisfy your requirements.

Our PDF files Understanding Network Forensics Analysis In An Operational are meticulously curated and chosen to use important insights and info to our customers. We have teamed up with professionals in various areas to make certain that our collection stays up-to-date and relevant.

From scientific research documents to educational resources, our PDF data cover a variety of subjects and topics. With very easy access to our collection, you can quickly check out and uncover the PDF Understanding Network Forensics Analysis In An Operational that interest you one of the most.

Our system is dedicated to providing you with a smooth and reliable means to boost your understanding and study experience. We comprehend the significance of having trusted and useful resources available, and that's why our PDF collection is continuously growing and increasing.

So whether you're a trainee, specialist or simply curious, exploring our extensive collection of PDF files Understanding Network Forensics Analysis In An Operational makes certain to supply you with beneficial understandings and expertise. Start surfing today to uncover exciting brand-new research opportunities!

BASIC STEPS TO DOWNLOADING AND INSTALL UNDERSTANDING NETWORK FORENSICS ANALYSIS IN AN OPERATIONAL PDF

Cyber Crime and Forensic Computing Walter de Gruyter GmbH & Co KG

Keeping up with the latest developments in cyber security requires ongoing commitment, but without a firm foundation in the principles of computer security and digital forensics, those tasked with safeguarding private information can get lost in a turbulent and shifting sea. Providing such a foundation, Introduction to Security and N

Network Forensics CRC Press

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to

detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today’s organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders’ abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

System Forensics, Investigation, and Response Elsevier Inc.

Chapters

The second edition of this comprehensive handbook of computer and information security provides the most complete view of computer security and privacy available. It offers in-depth coverage of security theory, technology, and practice as they relate to established technologies as well as recent advances. It explores practical solutions to many security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. The book is organized into 10 parts comprised of 70 contributed chapters by leading experts in the areas of networking and systems security, information management, cyber warfare and security, encryption technology, privacy, data storage, physical security, and a host of advanced security topics. New to this edition are chapters on intrusion detection, securing the cloud, securing web apps, ethical hacking, cyber forensics, physical security, disaster recovery, cyber attack deterrence, and more. Chapters by leaders in the field on theory and practice of computer and information security technology, allowing the reader to develop a new level of technical expertise Comprehensive and up-to-date coverage of security issues allows the reader to remain current and fully informed from multiple viewpoints Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Network Forensics Springer Nature

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

A Practical Guide to Computer Forensics Investigations Jones & Bartlett Learning

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 investigations Gather

intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10–specific feature forensics Utilize 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

Network Forensics Pearson Education

An authoritative guide to investigating high-technologycrimes Internet crime is seemingly ever on the rise, making the needfor a comprehensive resource on how to investigate these crimeseven more dire. This professional-level book--aimed at lawenforcement personnel, prosecutors, and corporateinvestigators--provides you with the training you need in order toacquire the sophisticated skills and software solutions to stay onestep ahead of computer criminals. Specifies the techniques needed to investigate, analyze, anddocument a criminal act on a Windows computer or network Places a special emphasis on how to thoroughly investigatecriminal activity and now just perform the initial response Walks you through ways to present technically complicatedmaterial in simple terms that will hold up in court Features content fully updated for Windows Server 2008 R2 andWindows 7 Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academicadoption, Mastering Windows Network Forensics and Investigation,2nd Edition offers help for investigating high-technologycrimes.

At our platform, our team believe in making the process of downloading PDF documents Understanding Network Forensics Analysis In An Operational fast and problem-free. Right here's just how you can access and download PDFs free of charge:

Action 1: Check out our comprehensive collection of PDF data to locate the one you need.

Action 2: Click the download button beside the PDF Understanding Network Forensics Analysis In An Operational you want to save.

Action 3: Wait for the PDF file Understanding Network Forensics Analysis In An Operational to download and install to your tool. This must just take a couple of seconds.

Which's it! You can now access Understanding Network Forensics Analysis In An Operational PDF file offline any time and share it with others if you want.

Our team believe that discovering and investigating should be a straightforward and available experience for all. That's why we offer our service free of charge, making certain that you can access the info you require with no barriers.

ELEVATE YOUR LEARNING AND RESEARCH

At our system, our team believe that education ought to be accessible to all. That's why we provide a substantial collection of

PDF downloads including **Understanding Network Forensics Analysis In An Operational** that cater to a variety of interests and subjects. Our educational resources are best for pupils, specialists, and anyone wanting to expand their knowledge.

With our PDF downloads, you can access beneficial details on numerous subjects, including background, scientific research, modern technology, and off course Understanding Network Forensics Analysis In An Operational. Our sources are excellent for research study functions and can aid you strengthen your understanding of complicated topics.

Our library is frequently growing, and we make every effort to include brand-new and pertinent material consistently. With our easy to use interface, you can conveniently navigate our system and discover the most up to date instructional resources.

By downloading Understanding Network Forensics Analysis In An Operational, you can boost your learning and research study ventures and acquire beneficial insights that can profit you in your personal and specialist life.

So, what are you awaiting? Start exploring our collection today and unlock a world of understanding within your reaches.

FINAL THOUGHT

At our platform, we make every effort to offer a hassle-free and complimentary solution that enables you to download Understanding Network Forensics Analysis In An Operational from our huge collection easily. Our user-friendly user interface guarantees that you can access the info you need without any difficulties or challenges.

Whether you're a student, expert, or just curious, our PDF downloads offer useful educational sources that can enrich your expertise and understanding of various subjects. By discovering our substantial collection, you can expand your discovering and research endeavors and elevate your understanding of the globe around you.

So why wait? Begin downloading and install **Understanding Network Forensics Analysis In An Operational** and start exploring our library today and unlock a globe of expertise within your reaches. Whether you're looking to expand your perspectives or carry out study, our uncomplicated and complimentary solution is right here to support you every action of the method.

Anatomy of Common UC Attacks Cisco Press

Cyberforensics is a fairly new word in the technology our industry, but one that n- ertheless has immediately recognizable meaning. Although the word forensics may have its origins in formal debates using evidence, it is now most closely associated with investigation into evidence of crime. As the word cyber has become synonymous with the use of electronic technology, the word cyberforensics bears no mystery. It immediately conveys a serious and concentrated endeavor to identify the evidence of crimes or other attacks committed in cyberspace. Nevertheless, the full implications of the word are less well understood. Cyberforensic activities remain a mystery to most people, even those fully immersed in the design and operation of cyber te- nology. This book sheds light on those activities in a way that is comprehensible not only to technology professionals but also to

the technology hobbyist and those simply curious about the ?eld. When I started contributing to the ?eld of cybersecurity, it was an obscure ?eld, rarely mentioned in the mainstream media. According to the FBI, by 2009 organized crime syndicates were making more money via cybercrime than in drug traf?- ing. In spite of the rise in cybercrime and the advance of sophisticated threat actors online, the cyber security profession continues to lag behind in its ability to inves- gate cybercrime and understand the root causes of cyber attacks. In the late 1990s I worked to respond to sophisticated attacks as part of the U. S.

Privacy and Security Jones & Bartlett Learning

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Practically every crime now involves some digital evidence; digital forensics provides the techniques and tools to articulate this evidence. This book describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

The Best Damn Cybercrime and Digital Forensics Book Period Academic Press

Keeping up with the latest developments in cyber security requires ongoing commitment, but without a firm foundation in the principles of computer security and digital forensics, those tasked with safeguarding private information can get lost in a turbulent and shifting sea. Providing such a foundation, Introduction to Security and Network Forensics covers the basic principles of intrusion detection systems, encryption, and authentication, as well as the key academic principles related to digital forensics. Starting with an overview of general security concepts, it addresses hashing, digital certificates, enhanced software security, and network security. The text introduces the concepts of risk, threat analysis, and network forensics, and includes online access to an abundance of ancillary materials, including labs, Cisco challenges, test questions, and web-based videos. The author provides readers with access to a complete set of simulators for routers, switches, wireless access points (Cisco Aironet 1200), PIX/ASA firewalls (Version 6.x, 7.x and 8.x), Wireless LAN Controllers (WLC), Wireless ADUs, ASDMs, SDMs, Juniper, and much more, including: More than 3,700 unique Cisco challenges and 48,000 Cisco Configuration Challenge Elements 60,000 test questions, including for Certified Ethical Hacking and CISSP® 350 router labs, 180 switch labs, 160 PIX/ASA labs, and 80 Wireless labs Rounding out coverage with a look into more advanced topics, including data hiding, obfuscation, web infrastructures, and cloud and grid computing, this book provides the fundamental understanding in computer security and digital forensics required to develop and implement effective safeguards against ever-evolving cyber security threats. Along with this, the text includes a range of online lectures and related material, available at: http://asecuritybook.com.

Computer and Information Security Handbook Springer

Annotation A comprehensive and broad introduction to computer and intrusion forensics, covering the areas of law enforcement, national security and corporate fraud, this practical book helps

professionals understand case studies from around the world, and treats key emerging areas such as stegoforensics, image identification, authorship categorization, and machine learning.

Computer and Intrusion Forensics Packt Publishing Ltd

Part of the Jones & Bartlett Learning Information Systems Security & Assurance Series! System Forensics, Investigation, and Response, Third Edition examines the fundamentals concepts readers must know as they prepare for a career in the cutting-edge field of system forensics.

The Digital Forensics Guide for the Network Engineer Artech House

This book primarily focuses on providing deep insight into the concepts of network security, network forensics, botnet forensics, ethics and incident response in global perspectives. It also covers the dormant and contentious issues of the subject in most scientific and objective manner. Various case studies addressing contemporary network forensics issues are also included in this book to provide practical know – how of the subject. Network Forensics: A privacy & Security provides a significance knowledge of network forensics in different functions and spheres of the security. The book gives the complete knowledge of network security, all kind of network attacks, intention of an attacker, identification of attack, detection, its analysis, incident response, ethical issues, botnet and botnet forensics. This book also refer the recent trends that comes under network forensics. It provides in-depth insight to the dormant and latent issues of the acquisition and system live investigation too. Features: Follows an outcome-based learning approach. A systematic overview of the state-of-the-art in network security, tools, Digital forensics. Differentiation among network security, computer forensics, network forensics and botnet forensics. Discussion on various cybercrimes, attacks and cyber terminologies. Discussion on network forensics process model. Network forensics tools and different techniques Network Forensics analysis through case studies. Discussion on evidence handling and incident response. System Investigations and the ethical issues on network forensics. This book serves as a reference book for post graduate and research investigators who need to study in cyber forensics. It can also be used as a textbook for a graduate level course in Electronics & Communication, Computer Science and Computer Engineering.

REVIEW OF UNDERSTANDING NETWORK FORENSICS ANALYSIS IN AN OPERATIONAL

• I keep a mental list of my favorite books I have read. Eragon is currently at a tie for first. Who is it tied with you ask? None other than Eldest, book two of the Inheritance Trilogy by Christopher Paolini, the same series to which Eragon belongs. I am sure that the third book (unreleased and untitled at time of this review) will also be #1, wether it will be tied for first with the ither two, or ahead of them I am not sure. I can't wait for Eragon the movie which is in production as i type this.http://www.eragonmovie.com

• I love Harry Potter Books and a lot more other teen novels such as the Bronze Bow. However, this book is very dull and I agree with others who say it is a rip off from other novels. I have read five chapters and I am, not sure if I want to go on. This was said

to be as good as harry potter but I think it is very poor work.