DOWNLOAD PDF INTRODUCTION TO CYBER SECURITY BOOK

Chapter 1 : 10 Must-Read Books for Information Security Professionals

Most introductory books on cyber security are either too technical for popular readers, or too casual for professional ones. This book, in contrast, is intended to reside somewhere in the middle.

Common Vulnerabilities[edit] Vulnerabilities in Cybersecurity system can come from many different factors. Thus, creates more opportunities for attacks to make their mark. Also, whenever user input is a variable, there can be ways into a system. This is because it is difficult for a programmer to predict and account for all possible inputs from a user. Denial of service attacks[edit] Denial of service DoS attack is a type of cyber attack that floods a network with multiple requests of information with the purpose of shutting down or disrupting services of a host connected to the internet. It may also prevent users of a service running through the targeted server or network. Direct-access attacks[edit] This form of vulnerability is when a system is physically accessed by an unauthorized user. This allows the user to make modifications or attach backdoor hardware or software in order to access the system remotely. The unauthorized user can also make complex changes to the system due to having direct access to the hardware. Hackers can use pharming by using tools that redirects users to a fake site. The victimized users will go to a fake website without noticing it is fake. Social Engineering[edit] Social engineering involves human interaction and the manipulation of people to give up confidential information. The purposes for this technique include fraud, system access or information gathering. It is easier for someone to fool you into giving them a password or bank information than it is for someone to try hacking in order to get the information. Other Vulnerabilities[edit] There are other vulnerabilities and ways that hackers can gain access of a system. They can use backdoors which is a different method of accessing a computer or network that bypass the authentication and security. Spoofing can also be used to trick a receiver by pretending to be a known source to the receiver. A more complicated one is clickjacking. Designed in secret, Stuxnet is designed to target the simple logic controllers found in most heavy machinery, including nuclear centrifuges. Stuxnet was specifically designed to attack Iranian nuclear centrifuges and management equipment, physically destroying them by altering core operating processes while reading an "all clear" signal to any command and control devices. Some say Stuxnet was too effective, as it now exists in the World Wide Web, capable of silently infecting a device and destabilizing it to the point of physical damage. The email would possess a subject titled "I Love you" and a text file called "Love Letter. Once activated, Zeus would perform several criminal activities towards users. Zeus is known for key-logging, data mining, and form grabbing. It is also used as a backdoor to install several other destructive pieces of malware, including ransom-ware and botting programs. Zeus is still actively spreading today and is very difficult to detect, even with proper antivirus installed. Currently, it is unknown how many PCs are infected with Zeus, but it is known as the largest, most powerful BotNet in the world. The FBI announced that hackers in the Eastern Europe had managed to infect computers around the world using the Zeus virus in October Zeus was distributed in an email that targeted individuals at businesses, once the email was opened, the trojan software would essentially install itself on the victims computer. Once installed, the virus would secretly capture passwords, account numbers, and other data that is need to log into online banking accounts. The hackers would then route the funds to other accounts controlled by a network of money mules. Large amounts of the money mules were recruited from overseas. They would then create false bank accounts using fake documents and false names. Once the money was in the accounts, the mules would either wire the money to their bosses in Eastern Europe, or withdraw it in cash and smuggle it out of the country. The Morris Worm[edit] The Morris Worm was created with the innocent meaning to see how big cyberspace was. After a while the worm had a critical error and "morphed" into a virus that spread to over computers and caused almost million dollars in damages. The Morris worm contributed greatly to the current measures used today to prevent DdoS attacks. The Ashley Madison Attack[edit] In a group called the Impact Team gained access to the Ashley Madison, a dating website for affairs, user information database. Many politicians were shamed after having their emails turn up in the dump and some people even committed suicide after being exposed. This attack took down many high-profile sites such as Twitter, Netflix, and several others. The attack resulted

in the website being shutdown for several minutes. They are the core concepts on which to base the development of security systems. The components of AAA are access control, authentication, and accounting. Access control is the management of how users can interact with the system, or what resources they can access. These consist of administrator settings. Authentication is most often seen as a password but is any way of verifying the identity of a user before allowing them to access the system. Accounting is the record keeping of what users do while connected to the system. These allow the protection of the system from access by unwanted users, limiting how they can access the system, and being able to track what happens on the system. Though these concepts do not work to eliminate permeated security threats, they serve as a basic protection. The degree to which these methods are applied is up to the organization, and there are countless different resources and kinds of protections for cyber-security systems. Authentication is a process used by a server when it needs to know exactly who is accessing trying to access information or website that its present on the particular server. Authentication can be done in several ways but the most common way of authentication is the input of a username and password into a certain system. Another means of authentication could be through the use of PIN. Authorization is the process of verifying access to a system has been granted. Again with the technical support example. Once the operator is able to input the PIN into the system, he gets access and can help the customer with the troubleshoot. Authorization[edit] Authorization is a process that a server uses to determine whether or not a client has permission to use a resource or access a file within that server. It compares the credentials provided with the credentials on file in the server database. Authorization usually goes hand-in-hand with authentication because the server needs to have some sort of concept of what client is requesting permission. Sometimes there is no authorization which means that any user may be able to use a resource or access a file by just asking for it. For example, most of the web pages on the Internet that most people use today require no type of authentication or authorization. Passsword authentication can be a problem, because some passwords are easy to guess and can be compromised without a problem. This is what lead to the two-factor authentication. It takes what you know - a password and username - and it takes what you have, possession factor that usually provides some code that is unique to you and only you can see for a short time. A lot of websites are upgrading their security by implementing these factors. Auditing[edit] A security audit is an evaluation of security in an information system. Security audits prevent cyber-crime by providing a persistent way of keeping track of what files were accessed, by who, and when. Security Audits are commonly performed by Federal or State Regulators, Corporate Internal Auditors, Consultants, and External Auditors â€" who are all either specialized accountants or technology auditors. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information. In December , the GOP group demanded that Sony pull its film The Interview, a comedy about a plot to assassinate North Korean leader Kim Jong-un, and threatened terrorist attacks at cinemas screening the film. Furthermore, two other high-ranking members of the LOD confirmed that the "Great Hacker War" never occurred, reinforcing the idea that this was just a competition of one-upsmanship. And the one-upsmanship was not matched evenly on both sides, in fact if this was a "war", it was not a fight at all. LulzRaft[edit] LegionData is the name of a computer hacker group or individual that gained international attention in due to a series of high-profile attacks on Canadian websites. The hackers posted an alert on the site claiming that Harper had choked on a hash brown while eating breakfast and was airlifted to Toronto General Hospital. A spokesman for the Prime Minister soon denied the story. The information accessed by the group including the names of donors as well as their home and e-mail addresses. LulzRaft later stated that the party had "terrible security" and that for the intrusion it used very basic methods. LulzRaft also apparently hacked into the website of Husky Energy on the same day. They inserted a notice promising free gas to users who used the coupon code "hash-browns", claiming that it was a gesture of goodwill intended to placate conservatives who were offended by their previous attacks. The Pentagon spent nearly 14 months cleaning the worm, named agent. In order to try and stop the spread of the worm, the Pentagon banned USB drives, and disabled Windows autorun feature.

Chapter 2 : Introduction to cyber security: stay safe online by The Open University

"Introduction to Computer Networks and Cybersecurity is much more than an introductory book. It is a well written, organized, and comprehensive book regarding the security in the Internet.

Practical considerations Design instrumentalities Another naive, but sadly common, method of advancing cybersecurity science is by uninformed and untested guessing. We guess about what users want tools to do. We guess about what to buy and how to deploy cybersecurity solutions. Guessing is uninformed and ineffective, and while it may appear to advance security, it is difficult to defend and often fails miserably. Unfortunately, science has a reputation for being stuffy and cold, and something that only people in white lab coats are excited about. As a cybersecurity practitioner, think of science as a way to explore your curiosity, an opportunity to discover something unexpected, and a tool to improve your work. You benefit every day from the experimentation and scientific investigation done by people in cybersecurity. To cite a few examples: Microsoft Research provides key security advances for Microsoft products and services, including algorithms to detect tens of millions of malicious Hotmail accounts. Government and private researchers created Security-enhanced Linux. Research at Google helps improve products such as Chrome browser security and YouTube video fingerprinting. Symantec Research Labs has contributed new algorithms, performance speedups, and products for the company. Cybersecurity is an applied science. That is, people in the field often apply known facts and scientific discoveries to create useful applications, often in the form of technology. Other forms of science include natural science e. Cybersecurity overlaps and is influenced by connections with social sciences such as economics, sociology, and criminology. What About the Art of Cybersecurity? There is art in becoming an expert at reverse engineering and malware analysis because skill, practice, and experience make practitioners better at those tasks. However, the art and practice of password management leads to different conclusions. Password strength is based on mathematical properties of the encryption algorithms used and the strength of modern computers. Art is one way to handle the ever-changing assumptions and landscape in cybersecurity. Take address space layout randomization ASLR , for example. ASLR is a technique of randomizing code in memory to prevent buffer overflow attacks. Researchers have been studying the effectiveness and shortcomings of this technique for years. One frequently cited paper from experimentally showed a way to de-randomize memory even under ASLR. This example illustrates the change in knowledge over time. For example, if you wanted to figure out how to tune your intrusion detection system, that could be an applied research project. The Importance of Cybersecurity Science Every day, you as developers and security practitioners deal with uncertainty, unknowns, choices, and crises that could be informed by scientific methods. You might also face very real adversaries who are hard to reason about. The highest priority should be assigned to establishing research protocols to enable reproducible experiments. Your job is defending your corporate network and you have a limited budget. Game theory is a scientific technique well-suited to modeling the arms race between attackers and defenders, and quantitatively evaluating dependability and security. As a malware analyst, you are responsible for writing intrusion detection system IDS signatures to identify and block malware from entering your network. You want the signature to be accurate, but IDS performance is also important. If you knew how to model the load, you could write a program to determine the number of false negatives for a given load. You decide to run analysis to determine whether people will buy your software, by comparing the number of compromises when using your product versus antivirus and also factoring in the cost of the two products. However, users have started complaining about the app crashing randomly. Cybersecurity requires defenders to think about worst-case behaviors and rare events, and that can be challenging to model realistically. Cybersecurity comprises large, complex, decentralized systemsâ€”and scientific inquiry dislikes complexity and chaos. Cybersecurity must deal with inherently multiparty environments, with many users and systems. Accordingly, it becomes difficult to pinpoint the important variable s in an experiment with these complex features. Cybersecurity is complex because it is constantly changing. Amazon, which has reportedly sold as many as items per second, commissioned a study to determine how many different shaped and sized boxes they needed. The mostly

mathematical study went on for over a year and the team produced a recommendation. Cybersecurity, like shopping habits, is a constantly changing problem, as evidenced by dynamic Internet routing and the unpredictable demand on Internet servers and services. Instead of proving a scientific hypothesis correct, the idea is to disprove a hypothesis. Popper used falsifiability as the demarcation criterion for science but noted that science often proceeds based on claims or conjectures that cannot easily be verified. It means that if the hypothesis were false, then you could demonstrate its falsehood. Perhaps it is based on undisclosed evidence. If the statement is wrong, all you will ever find is an absence of evidence. There is no way to empirically test the hypothesis. Central motivations for the scientific method are to uncover new truths and to root out error, common goals shared with cybersecurity. Businesses need new products and innovations to stay alive, and science can produce amazing and sometimes unexpected results to create and improve technology and cybersecurity. Science can also provide validation for the work you do by showingâ€"even provingâ€"that your ideas and solutions are better than others. If you choose to present your findings in papers or at conferences, you also receive external validation from your peers and contribute to the global body of knowledge. Think about how much science plays a part at Google, even aside from security. Today, Google researchers publish dozens of papers on security every year and those results inform security in their products and services, from Android to Gmail. Scientific advances conducted inside and outside the company undoubtedly save and make money for Google. Lastly, learning science consists, in part, of learning the language of science. The Scientific Method The scientific method is a structured way of investigating the world. This group of techniques can be used to gain knowledge, study the state of the world, correct errors in current knowledge, and integrate facts. Importantly for us, the scientific method contributes to a theoretical and practical understanding of cybersecurity. At its heart, the scientific method contains only five essential elements: Formulating a question from previous observations, measurements, or experiments Induction and formulation of hypotheses Making predictions from the hypotheses Experimental testing of the predictions Analysis and modification of the hypotheses These steps are said to be systematic. That is to say, they are conducted according to a plan or organized method. If you jump around the steps in an unplanned way, you will have violated the scientific method. There are also five governing principles of the scientific method. A fair, objective experiment is free from bias and considers all the data or a representative sample , not just data that validates your hypothesis. It must be possible to show that your hypothesis is false. It must be possible for you or others to reproduce your results. The results from the scientific method can be used to predict future outcomes in other situations. Nothing is accepted until verified through adequate observations or experiments. However, the problem may be systemic. Take performance, for example. Say you have a malware detection tool and want to analyze 1, files. It might be, but it masks implementation details that actually matter to the amount of wall clock time the algorithm takes in practice. There are many research designs to choose from in the scientific method. The one you pick will be primarily based on the information you want to collect, but also on other factors such as cost. Types of output for various research methods Research method.

Chapter 3 : Get Started Today In Introduction to Cybersecurity | Networking Academy

Understand Cyber Attacksâ€"and What You Can Do to Defend against Them This comprehensive text supplies a carefully designed introduction to both the fundamentals of networks and the latest advances in Internet security.

Learn more about J. He has been the principal investigator on research projects funded by NSF, the U. His current research interests include cybersecurity. He is an author and co-author of two books, 58 journal papers, and more than conference publications. He also holds five U. He is the author or co-author of numerous publications, including 17 textbooks. He is the recipient of numerous education and technical awards. Reviews "Introduction to Computer Networks and Cybersecurity is much more than an introductory book. It is a well written, organized, and comprehensive book regarding the security in the Internet. The authors present analytically a useful manual concerning wireless security, malware defense, and the applications in Web security. The book helps readers to follow their own paths of learning while it is structured in distinctive modules that allow for flexible reading. It is a well-informed, revised, and comprehensible educational book that addresses not only professionals but also students or anybody else interested in cyber security and needs an integrated source. A Global Perspective April "This book touches every corner of the topic of computer network and cybersecurity. It explains thoroughly the concept of network layers. There are detailed instructions and illustrations on the design of each network layer employing the newest Cisco technology. In addition, the book discusses the security issues in the context of computer networks. Then it presents different prevention algorithms and techniques, starting with cryptographic techniques. The strength of the book lies in the fact that it also includes the recent and emerging Internet Engineering Task Force and Institute of Electrical and Electronic Engineers standards and drafts that govern computer network and security technologies. Both the Instructor and the students would be able to maintain an up-to-date knowledge on the state-of-the-art technologies regarding network security. The text book presents a comprehensive overview of the fundamental concepts as well as state-of-the-art technologies in computer networks and security in cyber domain. The modular structure of the book makes it easy to adapt it for a variety of programs, including computer engineering, computer science, computer networks, computer security, and security systems, with different student backgrounds. The reader can quickly identify and learn about various cyber attacks, and become familiar with terminology of attacks, authentication, and protocols chain of trust, phishing attacks, cross-site request forgery attacks, bonnet attacks, DNSSEC, DKIM, SNMP, â€¦. The coupling of networking protocols and networks with their corresponding cybersecurity issues is a very good idea. This is an excellent text, content is very refreshing, informative, and easy to follow for students ranging from novice to advanced levels. It contains an impressive collection of up-to-date cybersecurity issues and analysis.

Chapter 4 : Introduction to Computer Networks and Cybersecurity - pdf - Free IT eBooks Download

Some good sites to get started are Microsoft Virtual Academy (they have a course on cyber security that is supposed to help you get certified by them: Security Fundamentals) and Coursea (a variety of IT related courses). As for books there are many, its a good idea to go to a bookstore and just flip through a bunch of them to see which you like.

November 23, by Jeremiah Talamantes While some security breaches are out of our control e. We could have stopped or prevented them from happening. These fake engineers will say something along these lines to their victims: I tend to stay away from technical books because I find so many are poorly written and inaccurate, but this one was full of great information. When I was developing courses for Fanshawe College, I selected the third edition of this book as a textbook. It lent itself incredibly well to learning the basics of and gaining a solid foundation in information security. Ghost In the Wires: From spending all night dial-up breaking into phone systems to convincing company employees into installing malicious programs from diskettes sent via snail mail, this book excellently captures the pulse of a genuinely gifted social engineer. His actions invoke criminal charges, ultimately leading him to go on the run. Thought of as a tenet in cybersecurity, people are the first line of defense for any corporate security program. This non-technical book is a must read for an intriguing perspective into securing the human behind the keyboard. Hacking Exposed , now in its seventh edition, is still a great introduction into the basics of network attack and defense. Reflecting the evolving need for more specialist focus in different areas, its recognised brand has now of course diversified into editions for mobile, ICS, rootkits, Linux, Windows, wireless, and you name it. I first bought the second edition of Hacking Exposed back in , and it immediately changed the way I was thinking about the systems for which I was then responsible. Whilst much of the technology specifics in that edition will now seem quaintly retro, it is both sobering and more than little disheartening to see how some of the actual techniques are still in active use today. It is always great to have as many technical skills as you can possibly learn. Those are the skills that will get you the InfoSec job you desire, but you also have to be able to communicate your ideas in a way that not only instructs but also makes the audience want to hear more. You need a way that makes people want to engage with you. You need a course in charisma! It offers exercises and techniques that can transform even the most socially inept InfoSec person into someone who can better connect with an audience. It is nice to know how all the exploits work and why it matters to be more security conscious. The technology in this book might have changed, but the concepts are still the same. In order to properly defend the confidential data within your network, there needs to be proper extrusion detection in place to detect intruders who have comprised your internal systems and siphoned out sensitive data. This book gives you some serious food for thought on how this can be applied to your network.

Chapter 5 : Introduction to Computer Networks and Cybersecurity - CRC Press Book

SecureWorks, an information security service provider, reported in that the United States is the "least cyber-secure country in the world," with attacks per computer during the previous year - compared with just attempted attacks per computer in England.

Chapter 6 : Intro to Cybersecurity - - The Cisco Learning Network

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Chapter 7 : Introduction to Cybersecurity Science - Essential Cybersecurity Science [Book]

Introduction to cyber security has 5 ratings and 0 reviews. This hour free course introduced online security: how to recognise threats and take steps.

DOWNLOAD PDF INTRODUCTION TO CYBER SECURITY BOOK

Chapter 8 : Introduction to Information Technology/Cybersecurity - Wikibooks, open books for an open wor

Introduction to Cyber Security. Our lives depend on online services. Gain essential cyber security knowledge and skills, to help protect your digital life.