Cyber Security Overview for Absolute Beginners

A beginner's guide to Cyber Security

FARHADUR RAHIM

ISBN: 9798790401183

WHAT WILL YOU LEARN?

In Chapter 1, you will learn on the internet so call cyber space.

In Chapter 2, you will learn about hackers, classification or categories of hackers, understanding cracker.

In Chapter 3, you will learn about malwares, various purposes of malwares, types of malwares in cyber-attacks and similar use cases.

In Chapter 4, you will learn all about cybercrimes, categories, different types of cybercrimes, impact in our society.

In Chapter 5, you will learn about authentication in cybersecurity. Ensuring digital identity and security understanding authentication, The importance of authentication, methods of authentication, authentication in action.

In Chapter 6, you will learn in detail about encryption in cybersecurity, how does encryption work, benefits and use cases.

In Chapter 7, you will learn about digital signatures in cybersecurity, The consequence of digital signatures, applications in real-world.

In Chapter 8, you will learn about Antivirus in Cybersecurity, The importance of antivirus, applications in real-world.

In Chapter 9, you will learn about understanding firewalls, firewall mechanisms: how they work, the importance of firewalls: safeguarding digital frontiers applications in real-world.

In Chapter 10, you will learn about steganography and little more about the significances of steganography.

In Chapter 11, you will learn about investigating cybercrimes: introduction to computer forensic, computer forensic applications and impact, challenges and future trends.

In Chapter 12, you will learn about various certifications on cyber security. Learn about certified ethical hacker (CEH), Comptia Security+, CISSP and more.

DEDICATION

This book is dedicated to beginners who are interested in learning about cyber security and ethical hacking. This book is primarily intended for Application developers, Programmers, Software Engineers, DevOps, IT managers, technology architects, Teachers and Students who study in IT. If you are also ready to learn about new technologies, then this book is ideal for you.

To all those who tirelessly strive to protect the digital realm. Your dedication, attention, and expertise in the field of cyber security are an encouragement of hope in an interconnected world. May your efforts continue to boost our defenses, secure our data, and preserve the integrity of the digital landscape for generations to come.

CONTENTS

ACKNOWLEDGMENTS

Writing a book is a journey that involves the support, encouragement, and contributions of numerous individuals and entities. As I stand on the threshold of completing this endeavor, I am filled with gratitude for the many people who have made this book possible.

First and foremost, I would like to express my heartfelt gratitude to my family, whose unwavering love and understanding provided me with the time and space to bring my ideas to life. Your support has been a constant source of inspiration.

I extend my sincere appreciation to my friends and colleagues who provided valuable feedback, brainstormed ideas, and offered their insights throughout the writing process. Your perspectives have enriched the content of this book immensely.

I am immensely thankful to the experts and professionals who graciously shared their expertise and experiences, allowing me to present accurate and informed insights within these pages. Your willingness to share your knowledge is deeply appreciated.

A special acknowledgment goes to my mentor, whose guidance and wisdom have been invaluable on this journey. Your encouragement pushed me to strive for excellence in every chapter.

To the editorial and publishing teams who worked tirelessly to shape this book into its final form, I extend my gratitude for your dedication to quality and precision.

Last but not least, I would like to thank the readers, whose curiosity and interest in this book give purpose to my writing.

This book is a testament to the collective effort and support of all those mentioned above and many more whose names may not appear here. Your contributions, no matter how small, have left an indelible mark on this work. Thank you for being a part of this journey.

With sincere appreciation,

Farhadur Rahim

OVERVIEWS

Cybersecurity is the practice of protecting digital systems, networks, devices, and data from malicious attacks, unauthorized access, and potential threats. In an increasingly connected world, where technology is integral to our daily lives, understanding the basics of cybersecurity is essential for everyone, from individuals to businesses. This overview provides a foundational understanding of key concepts in cybersecurity for beginners.
With all of these developments, it is important to acquire the necessary background knowledge of the fundamentals of cybersecurity. While it involves good technical knowledge, it is still possible even for a complete computer novice to gain a thorough understanding of the concepts and properties of cybersecurity and its prop.

The book is written in a way that is easy to understand. The technical concepts have been developed and explained in such a way that they will not be confusing for beginners.

CHAPTER 1

INTRODUCTION TO CYBERSPACE

t is the interconnected realm of digital systems, networks, and information uals, businesses, and governments communicate, exchange data, and conduct s using electronic devices and the internet. It's a virtual environment that has bec part of modern society, shaping how we interact, learn, work, and entertain ourse

t is among the most important inventions of the 21 century which have affected Internet have crossed every barrier and have changed the way we used to talk, play op, make friends, listen to music, see movies, order food, pay bill, greet your frien anniversary, etc., you name it. And we have an app in place for that. It has facilit naking it comfortable. Gone are the days when we have to stand in a long queue fo phone and electricity bills. Now we can pay it at a click of a button from our h he technology have reached to an extent that we don't even require a computer fo t. Now we have Internet enabled smartphone TomTom's, et cetera, through which connected to our friends, family and office 24 by seven, not only Internet has si but also it has brought many things within the reach of the middle class by maki ective.

ot long back while making an IED or even an STD call, the eyes were stricken on t he calls were very costly IED and were used to pass on urgent messages only and outine communication was done using letters since it was a relatively very cheap.

t came, let us discuss the brief history of Internet and learn how this Internet was i
v it evolved to an extent that now we cannot think of our lives without it.

clusion, internet has transformed the way we live, work, and interact, edented opportunities for communication, innovation, and collaboration. Howeve e the benefits of this interconnected realm, it's important to be mindful of the ch urity concerns it presents. Balancing the advantages with responsible online behav curity practices is essential for harnessing the full potential of cyberspace.

story of internet:

w what the Cold War between USA and Russia gave to the world, but defiantly, the f those very useful inventions whose foundation was laid during Cold War of nis aunched the world's first satellite, Sputnik, into the space on 4th October 1957. T he victory of Russia over the cyberspace and as a counter step, Advanced Research , the research arm of Department of Defense United States, declared the lau NET Advanced Research Projects Agency network in early 1960s. This was an exper k and was designed to keep the computers connected to this network to communic ner, even if any of the node due to the bomb attack fails to respond. The first mess er the ARPANET, a packet switching network by Leonard Kleinrock Labor ity of California, Los Angeles, UCLA. You will be surprised to know that the first s sent over the Internet was lo actually. They intended to send work log in and o letters reached its destination at Second Network Node at Stanford Research I nd before the last three letters could reach the destination, the network was down oon the error was fixed and the message was resending it. The major test that ARI play is to develop rules for communication, i.e. protocols for communicati NET. The ARPANET in particular led to the development of protoc working, in which multiple separate networks could be joined into a network of ne ted in the development of the protocol suite, which specifies the rules for join nicating over ARPANET. Soon after, in 1986, and as Foundational Science Fou ne was created, two and five U.S. universities, computing centers were conne ns fat. NSFNET, the successor of ARPANET, become popular by 1990 and ARI commissioned. There were many parallel networks developed by other universi ountries like the United Kingdom. In 1965, National Physical Laboratory NGPL p ng switching network, Michigan Educational Research Information Tribe formed k in 1966, which was funded and supported by State of Michigan and the National tion NSF. France also developed a packet switching network no facilities in 1973.

ovided backbone even as popular among the corporate, to facilitate the commercia
work. The Senate was decommissioned in 1995 and now the Internet coul
rcial traffic. So, this was the history of Internet where it came from.

ecurity Models

section, we will learn about the CIA Triangle, Confidentiality, Integrity, and Ava
own as the CIA Triangle, which is a security model created to guide security
ntiality in an enterprise. The three elements of the CIA triangle of confidentiality, i
ilability are considered the three most important components of security. This info
very useful if you work in the IT field or are planning to enter the field.

entiality, confidentiality is the security principle that controls access to informati
d to ensure the wrong people cannot gain access to sensitive information while e
t people can access it. Access to information must be restricted only to those
zed to view the required data.

n be categorized according to the type and severity of damage that could happ
t fall into unauthorized hands. According to these categories, strict measures can
ented. Protecting confidentiality may also include special training for those wh
e data, including familiarizing authorized users with security risk factors and teachi
guard vulnerable data assets. In addition to training, strong passwords and passwor
actices must be used, as well as information about social engineering attacks to
om unwittingly avoiding proper data handling rules and potentially causing di

mple of a method used to ensure confidentiality is the use of data encryption to fa
ication is now becoming the